Twenty problem sets to learn Elementary Number Theory from Hardy and Wright

Gaurav Bhatnagar
Ashoka University
bhatnagarg@gmail.com
https://gauravbhatnagar.org

Ojas Kumar
Chennai Mathematical Institute
ojaskumar00@gmail.com

Sagar Shrivastava
School of mathematics,
Tata Institute of Fundamental Research,
Homi Bhabha Road, Mumbai 400005, India
sagars@math.tifr.res.in

Contents

The Rules iv

Problem Set 1. 1

Problem Set 2. 3

Problem Set 3. 5

Problem Set 4. 7

Problem Set 5. 10

Problem Set 6. 12

Problem Set 7. 15

Problem Set 8. 17

Problem Set 9. 20

Problem Set 10. 23

Problem Set 11. 25

Problem Set 12. 28

Problem Set 13. 31

Problem Set 14. 34

Problem Set 15. 37

Problem Set 16. 41

Problem Set 17. 44

Problem Set 18. 47

Problem Set 19. 51

Problem Set 20. Test 54

The Rules

This document contains the problem sets made for a course in Elementary Number Theory. We follow a discovery approach. Every day, you will get a problem set with 25 problems. You are supposed to do them all (on your own) and write your solutions neatly. In the lectures we may discuss definitions and theorems which you may have already discovered (and proved) on your own, in earlier problem sets. Tutorials are for discussing difficulties.

Here are the rules.

(1) There will be a large number of calculations. Do them by hand. A common hand calculator is allowed. No sage.
(2) Write down the solutions neatly.
(3) Do problems in order.
(4) Finish them before the next day.
(5) DO NOT LOOK AT THE INTERNET OR REFER TO ANY BOOK UNTIL WE ASK YOU TO.
(6) You may discuss difficulties with each other, but only after trying the problems yourself.
(7) You have to do ALL the problems in the problem set.
(8) Begin Problem Set k+1 only after doing Problem Set k.

Notation. We denote by $\mathbb{N}$ the set consisting of the *natural numbers* 1, 2, 3, ... We also use the notation

$$\mathbb{N}_0 := \mathbb{N} \cup \{0\} = \{0, 1, 2, \dots\}.$$

We use $\mathbb{Z}$ for the set of integers.

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}.$$

We shall take for granted the notation of sets: $a \in A$ means a is an element of A, ϕ denotes the empty set, $\cup$ and $\cap$ are used for unions and intersections.

PROBLEM SET 1

1.1. Use a rectangular grid of dots to represent the multiplication 4×7.

1.2. Use dots to divide 27 by 5; 17 dots can be broken into groups of 5, and some dots are left over. Identify q and r where $27 = 5q + r$.

1.3. Use a rectangular grid of dots to represent the multiplication 7^2. Can you tell why this is read 'seven square'?

1.4. List the first 21 squares; i.e., list n^2, for $n = 0, 1, \ldots, 20$.

1.5. Calculate $1 + 3 + \cdots + 2n - 1$ for $n = 1, 2, 3, 4, 5$.

1.6. With 15 dots, how many rectangles of size $m \times n$ can you make? List all m, n such that $m \times n = 15$.

1.7. With 23 dots, how many rectangles of size $m \times n$ can you make? List all m, n such that $m \times n = 23$.

Definition 1.1 (Divisor)**.** We say $d \mid n$ (read d divides n, or d is a **divisor** of n) if there is an integer m such that $n = d \times m$. Another word used for divisor is **factor**.

Remark 1.2. The number 1 is a divisor of every natural number. By convention, any number n divides 0.

1.8. List all (positive) divisors of 15.

Note. Usually only positive divisors are considered.

1.9. List all (positive) divisors of 23.

Definition 1.3. A number $p > 1$ is a prime if the only divisors of p are 1 and p itself.

1.10. List all divisors of all the numbers from 1 to 20.

1.11. List all the primes smaller than 20.

1.12. Show that if $a \mid b$ and $b \mid c$ then $a \mid c$.

1.13. Show that if $n \mid a$ and $n \mid b$, then $n \mid a + b$.

1.14. Show that if $a \mid m$ and $a \mid n$ then for all x, y integers, $a \mid mx + ny$.

1.15. Show that a number $m > 1$ is either a prime or divisible by a number d, with $d < m$.

Remark. A number $n > 1$ which is not prime is said to be **composite**.

Proposition 1.4 (The well ordering principle (WOP)). *Let S be a non-empty subset of $\mathbb{N}$. Then S has a least element; i.e., there is an $r \in S$ such that $r \leq n$ for all $n \in S$.*

Remark. We will not prove WOP but take it for granted. We will show later that WOP is equivalent to the Principle of Mathematical Induction.

1.16. Write 12 as a product of primes.

1.17. Is 91 a prime?

1.18. Write 170 as a product of primes.

1.19. Write 360 as a product of primes.

1.20. List all divisors of 360.

1.21. Use WOP to show that any natural number $n > 1$ is a product of primes.

Definition 1.5. Let $n \in \mathbb{N}_0$. Then $n!$ is defined recursively as

$$0! = 1$$
$$n! = n \times (n-1)!$$

1.22. Calculate 6!.

1.23. Show that $4! + n$ is divisible by n for $n = 1, 2, 3, 4$.

1.24. Find three consecutive composite numbers.

1.25. Find 10 consecutive composite numbers.

PROBLEM SET 2

Definition 2.1 (GCD)**.** The **greatest common divisor** of two numbers n and m is a number d such that

(a.) $d \mid m$ and $d \mid n$.
(b.) d is the greatest with this property; i.e., if d' divides n and m, then $d' \leq d$.

We denote the GCD of two numbers n and m by (n, m).

2.1. What is $(5, 15)$?

2.2. Find $(7, 91)$.

2.3. If $m \mid n$, then what is (m, n)?

2.4. Write 18 and 24 as a product of prime factors.

2.5. Find $(18, 24)$ by using the above product form.

2.6. Find $(153, 795)$.

2.7. Find a number $n > 10$ such that $(5, n) = 1$ and a number $m > 10$ such that $(5, m) = 5$.

2.8. Let p be a prime and $n \in \mathbb{N}$. Show that $(p, n) = 1$ or $(p, n) = p$.

Theorem 2.2 (The Principle of Mathematical Induction)**.** *Let $S \subset \mathbb{N}$ such that*

(i.) $1 \in S$.
(ii.) If $k \in S$ then $k + 1 \in S$.

Then $S = \mathbb{N}$.

Note. A similar statement works for $\mathbb{N}_0$.

2.9. Prove Theorem 2.2 using WOP.

2.10. Let $O(n)$ be the sum of the first n odd numbers; i.e.,

$$O(n) = 1 + 3 + 5 + \cdots + (2n - 1).$$

Prove that $O(n) = n^2$.

2.11. Let $E(n)$ be the sum of the first n even numbers. Use the formula for $O(n)$ to find a formula for $E(n)$.

2.12. Let $T(n)$ be the sum of the first n numbers. Show that

$$T(n) = \frac{n(n+1)}{2}.$$

Note. You need to use induction for only one of the above three problems.

Remark. When d is a divisor of n, we say n is a **multiple** of d.

2.13. Find all natural numbers less than 20 that are multiples of 5.

2.14. Find all natural numbers less than 100 that are multiples of 11.

2.15. Find all positive multiples of 13 less than 100.

2.16. List the elements of the set

$$S = \{r \geq 0 \mid r = 3782 - 620k, k \in \mathbb{N}\}.$$

What is the least element of S?

2.17. Let m, n be two natural numbers, $n > m$, and

$$S = \{n - km \in \mathbb{N}_0 \mid k \in \mathbb{N}\}.$$

By WOP, S has a least element, say r. Show that if $r = 0$, then $m \mid n$.

Theorem 2.3 (Division algorithm)**.** *Given any two numbers m and n, there are numbers q and r such that $n = mq + r$, and either $r = 0$ or $0 < r < m$. The number q is called the* **quotient** *and r the* **remainder***.*

2.18. Convince yourself we have proved Theorem 2.3. Write this convincing argument.

Definition 2.4 (Congruence)**.** We say $a \equiv b \pmod{n}$ if $n \mid a - b$. This is read 'a is congruent to b mod n'.

Remark. The number a is congruent to b mod n if and only if they leave the same remainder when divided by n.

2.19. List the ten smallest, positive numbers congruent to 3 mod 5.

2.20. Write 5! as a product of prime numbers. Count the number of zeros it has.

2.21. How many numbers below 100 are divisible by 5?

2.22. How many numbers below 100 are divisible by 7?

Definition 2.5 (Greatest integer or floor function)**.** We use the notation $\lfloor x \rfloor$ to denote the greatest integer $n \leq x$.

Example 2.6. $\lfloor \frac{100}{5} \rfloor = 20$ and $\lfloor \frac{100}{7} \rfloor = 14$.

2.23. What is the remainder when $2 \times 3 \times 5 + 1$ is divided by 2, 3 or 5?

2.24. Let $p_1, p_2, \ldots, p_k$ be the first k primes. Let P be defined as

$$P = p_1 p_2 \cdots p_k.$$

Show that $P + 1$ when divided by p_i leaves remainder 1, for all $i = 1, 2, \ldots, k$.

Theorem 2.7 (Euclid)**.** *The number of primes is infinite.*

2.25. Prove Theorem 2.7.

PROBLEM SET 3

3.1. Simplify the following:

$$(1-x)(1+x),$$
$$(1-x)(1+x+x^2),$$
$$(1-x)(1+x+x^2+x^3).$$

3.2. Factor: x^3-1.

3.3. Factor: x^3+1.

3.4. Write 5 positive integers congruent to 3 mod 11.

3.5. List the ten smallest natural numbers congruent to 1 mod 4.

3.6. List the ten smallest natural numbers congruent to 3 mod 4.

3.7. Consider the arithmetic sequence

$$a, a+d, a+2d, \ldots, a+nd.$$

Show that

$$\sum_{k=0}^{n}(a+kd) = (n+1)a + d\frac{k(k+1)}{2}.$$

3.8. Verify that formula you found earlier for the sum of the first n odd numbers, by using this formula.

3.9. Find the sum of the first 10 positive numbers that are congruent to 3 mod 11.

3.10. Write 6 consecutive composite numbers.

3.11. Show that for any N, there is a set of N consecutive composite numbers.

3.12. Write the prime factorization of 10!.

3.13. What is a if $100! = 5^a m$, where 5 does not divide m; that is, what is the highest power of 5 that divides 100!?

3.14. Find the number of zeros at the end of 100!. That is, what is the largest number a such that 10^a divides 100!.

3.15. Show that if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

3.16. Show that if $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$.

3.17. Find all x such that $3x \equiv 1 \pmod{7}$. If no such x exists, then say so.

3.18. Find all x such that $3x \equiv 1 \pmod 6$. If no such x exists, then say so.

3.19. Find all x such that $3x \equiv 0 \pmod{12}$. If no such x exists, then say so.

3.20. Let

$$S = \{x + 2y \mid x, y \in \mathbb{Z}\}.$$

List all elements of S.

3.21. Let

$$S = \{2x + 3y \mid x, y \in \mathbb{Z}\}.$$

List all elements of S.

3.22. Let

$$S = \{2x + 4y \mid x, y \in \mathbb{Z}\}.$$

List all elements of S.

Definition 3.1. Let $n \in \mathbb{N}$. Define $n\mathbb{Z}$ to be the set of all the multiples of n. Here we allow multiples to be negative numbers.

3.23. Let a and b be two integers, not both zero.

$$S = \{ax + by \mid x, y \in \mathbb{Z}\}.$$

Let S^+ denote the positive numbers in S. Show S^+ is non-empty. By WOP, it has a least element, say d. Show that for all $s \in S$, $d \mid s$.

3.24. In the problem above, show that $d = (a, b)$.

Theorem 3.2. *Let a and b be two integers. Let $d = (a, b)$. Then the equation $ax+by = n$ has a solution if and only if $d \mid n$. In particular, there are x and y such that $ax+by = d$.*

Note. Convince yourself that we have already proved this theorem in the problems above.

3.25. Show that any common divisor of m and n divides $d = (m, n)$.

PROBLEM SET 4

4.1. Find x and y integers (if possible) such that $3x + 8y = 2$. If this is not possible, say why.

4.2. Find x and y integers (if possible) such that $3x + 6y = 2$. If this is not possible, say why.

4.3. Let $a > b$ be two positive numbers. Show that $(a, b) = (a - b, b)$ and $(a, a) = a$.

4.4. The Fibonacci sequence is defined by: $f_0 = 0$, $f_1 = 1$ and $f_{n+1} = f_n + f_{n-1}$. Write down f_n for $n = 0, 1, \ldots, 5$. Find (f_{n+1}, f_n) for $n > 1$.

Theorem 4.1. *Let p be a prime such that $p \mid ab$. The either $p \mid a$ or $p \mid b$.*

4.5. Prove Theorem 4.1. Note that to prove a statement of the form 'Either P or Q', you can assume 'Not P' and prove 'Q'. (Hint. When proving something, go over previously proved statements to get ideas on what you can use.)

4.6. Let $(a, b) = d$, and $c > 0$. Show that $(ac, bc) = dc$.

4.7 (Eratosthenes Sieve)**.** Find all the primes ≤ 100 by using the following technique. Begin by writing the numbers ≤ 100 as shown, and cross of the 1. Circle 2 and cross of all multiples of 2. Circle 3 and cross of all multiples of 3. Carry on in this fashion until all numbers are either circled or cancelled.

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Write down all the numbers that are circled. Argue that the numbers that are circled are all the primes less than or equal to 100.

4.8. Let n be a number. Show that if n is not prime then it is divisible by a prime p such that $p \leq \sqrt{n}$.

Remark. This shows that in computing the Eratosthenes sieve to find primes upto 100, we only need to cross off multiples of primes less that 10, i.e. until 7.

4.9. Factor 198 as a product of primes. Write the factors in **standard form**; that is, write the primes in increasing order so you get an expression of the form

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where p_1, p_2, ..., p_k are the distinct primes dividing 198, and $a_i > 0$.

4.10. Let $n = 3^3 5^2 11^7$ and $m = 3^2 5^5 7^3$. What is the largest power of 3 that divides both n and m?

4.11. Let n and m be as above. What is the smallest power of 5 that a common multiple of n and m must have?

Definition 4.2. We define $\mathbb{Z}_n$ as:

$$\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}.$$

This is called the **residue class mod** n.

Remark 4.3. Any number a is congruent to some r mod n, where r is one of 0, 1, 2, ..., $n-1$. So we say a is 'in the class of r modulo n'. The number r is simply a representative of that 'class'. For example, the integers congruent to 1 mod 4 are:

$$[1] := \{\ldots, -11, -7, -3, 1, 5, 9, \ldots\}.$$

This set's representative in $\mathbb{Z}_4$ is 1.

Note. In the following, find $x \in \mathbb{Z}_n$, for a suitable n.

4.12. Solve the equation $3x \equiv 1 \pmod{11}$. If no such x exists, then say so.

4.13. Solve the equation $x^2 \equiv -1 \pmod{7}$. If no such x exists, then say so. (Note that $-1 \equiv 6 \pmod{7}$, because $6 - (-1) = 7$ is divisible by 7.)

4.14. Solve the equation $4x \equiv 1 \pmod{7}$. If no such x exists, then say so.

4.15. Solve the equation $4x \equiv 1 \pmod{6}$. If no such x exists, then say so.

4.16. Solve the equation $7x \equiv 1 \pmod{18}$. If no such x exists, then say so.

4.17. Solve the equation $8x \equiv 1 \pmod{18}$. If no such x exists, then say so.

4.18. Calculate $3x \pmod{7}$ for all $x \in \mathbb{Z}_7$. (Your answers should be in $\mathbb{Z}_7$.)

4.19. Calculate $3x \pmod{8}$ for all $x \in \mathbb{Z}_8$.

4.20. Calculate $3x \pmod{9}$ for all $x \in \mathbb{Z}_9$.

4.21. Simplify:

$$(1-x)(1+x+x^2+\cdots+x^{17}).$$

4.22 (Geometric Sum)**.** Prove that

$$\sum_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x}.$$

4.23. Show that

$$x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}\right).$$

4.24 (Fermat numbers)**.** Let

$$F_n := 2^{2^n} + 1.$$

Compute F_1, F_2, F_3 and F_4.

4.25. Show that $F_n \mid F_{n+k} - 2$, for natural numbers n and k.

PROBLEM SET 5

Definition 5.1. Let A and B be sets. Define the set $A+B$ as the set of elements $a+b$ where $a \in A$ and $b \in B$.

5.1. Let $A = 2\mathbb{Z} = \{0, -2, 2, -4, 4, -6, 6, \dots\}$ and similarly, define $B = 3\mathbb{Z}$. Find $A+B$.

5.2. Find a d such that $6\mathbb{Z} + 9\mathbb{Z} = d\mathbb{Z}$.

5.3. Express 98 as a product of primes. Write the factors in standard form, as powers of distinct primes.

5.4. Express 350 as a product of primes in standard form.

Theorem 5.2 (Fundamental Theorem of Arithmetic)**.** *A number can be expressed in only one way as a product of primes in standard form; that is, apart from reordering the primes, there is only one way of expressing a number as a product of primes.*

5.5. Show that any number n can be written in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where p_1, p_2, …, p_k are the primes dividing n and $a_i > 0$.

5.6. Suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, and $n = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$, where the p_i's and q_i's are primes and a_i's and b_i's natural numbers. Here p_i's are distinct and q_i's are distinct. Show that $p_1 = q_j$ for some j.

5.7. Suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, and $n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where the p_i's are distinct primes. Show that $a_1 = b_1$.

5.8. Use the above to complete the proof of Theorem 5.2.

5.9. Find $(98, 350)$.

Definition 5.3. Let a and b be two numbers. The **least common multiple** of a and b, which we will denote by $[a, b]$ or $\operatorname{lcm}(a, b)$, is the number m such that:

(i.) $a \mid m$ and $b \mid m$.
(ii.) m is the smallest number with this property.

5.10. Find $[98, 350]$.

5.11. Let $m = p^3 q^2 r^7$ and $m = p^2 q^5 s^3$, where p, q, r, s are distinct prime numbers. What is the largest power of p that divides both n and m?

5.12. Let m and n be as above. What is the smallest power of q that a common multiple of n and m must have?

5.13. Let $n = 13^5 17^2 23^{12}$ and $n = 3^5 11^{12} 13^2$. Find (n, m) and $[n, m]$.

5.14. Consider the prime factorization of n^2. Suppose p^a comes in the prime factorization of n^2 in standard form. Argue that a is even.

5.15. Consider the prime factorization of $2m^2$. Suppose 2^a comes in the prime factorization of $2m^2$ in standard form. Argue that a is odd.

5.16. Find, if possible, n and m such that $2n^2 = m^2$, or show it is impossible.

5.17. Show that $\sqrt{2}$ is irrational; i.e., there are no integers m and n such that $\sqrt{2} = m/n$.

5.18. Find integers x and y such that $3x + 13y = 1$.

5.19. Find x in $\mathbb{Z}_{13}$ such that $3x \equiv 1 \pmod{13}$.

5.20. Find y in $\mathbb{Z}_3$ such that $13y \equiv 1 \pmod{3}$.

5.21. Find integers x and y such that $5x + 23y = 1$.

5.22. Find x in $\mathbb{Z}_{23}$ such that $5x \equiv 1 \pmod{23}$.

5.23. Let a and n be positive numbers such that $(a, n) = 1$. Show that there is an $x \in \mathbb{Z}_n$ such that $ax \equiv 1 \pmod{n}$.

5.24. Verify that $4x \equiv 1 \pmod{6}$ has no solution in $\mathbb{Z}_6$.

5.25. Let a and n be positive numbers such that $(a, n) > 1$. Show that there is no $x \in \mathbb{Z}_n$ such that $ax \equiv 1 \pmod{n}$.

PROBLEM SET 6

6.1. Let m, n be two numbers, $n > m$, and q and $r > 0$ such that $n = mq + r$. That is, on dividing n by m we get quotient q and remainder r, and r is not 0. Prove that $(n, m) = (m, r)$. However, if $r = 0$, then $(n, m) = m$.

Remark 6.1 (Euclid's algorithm to find GCD)**.** Problem 6.1 shows how one can use division to compute the gcd. Divide n by m. If remainder r is not 0, $(n, m) = (m, r)$. Thus the problem is reduced to finding the GCD of smaller numbers. In the next step, divide m by r. Suppose the remainder is r_1. If $r_1 = 0$, then the GCD is r, since $(m, r) = r$. Otherwise $(m, r) = (r, r_1)$. Continue this process until you obtain $r_{k+1} = 0$. The GCD of n and m is r_k (Why?). Note that the numbers n, m, r, r_1, r_2, ... keep decreasing, so at some point we have to get 0, and thus the process has to stop.

6.2. Find $(21, 6)$ using Remark 6.1, At each step corresponding to $n = mq + r$, find x and y such that $nx + my = r$. Finally, calculate backwards to find x and y such that $21x + 6y = d$, where $d = (21, 6)$.

6.3. Find $(72, 26)$ using Remark 6.1, At each step corresponding to $n = mq + r$, find x and y such that $nx + my = r$. Finally, calculate backwards to find x and y such that $72x + 26y = d$, where $d = (72, 26)$.

Example 6.2. We can encapsulate all the calculations involved in finding the GCD of two numbers in one object called a **continued fraction**. We do this by writing $n = mq + r$ as

$$\frac{n}{m} = q + \frac{r}{m} = q + \frac{1}{m/r}.$$

Now repeat the process with $\frac{m}{r}$. Here is an example.

$$\begin{aligned} \frac{17}{6} &= 2 + \frac{5}{6} \\ &= 2 + \frac{1}{6/5} \\ &= 2 + \frac{1}{1 + \frac{1}{5}} \end{aligned}$$

6.4. Find a continued fraction for $\frac{72}{26}$.

6.5. Find a continued fraction for $\frac{5}{3}$.

6.6. Find a continued fraction for $\frac{13}{8}$.

6.7. Find a continued fraction for $\frac{21}{13}$.

6.8. Consider numbers of the form a^n+1. Argue that if a is an odd number bigger than 1, then a^n+1 cannot be prime.

6.9. Show that a^6+1 is divisible by a^2+1, for any $a \in \mathbb{N}$.

6.10. Suppose $n = m \times k$, with $m > 1$ an odd divisor of n. Then show that a^n+1 is not prime. Argue that if a^n+1 is prime, then $n = 2^m$ for some m.

6.11. Suppose $n > 1$ and $a^n - 1$ is a prime. Show $a = 2$ and n is a prime.

Remark 6.3. Primes of the form 2^p-1, where p is prime, are called **Mersenne primes**.

6.12. Calculate the first four Mersenne primes.

6.13. Show that the product of two numbers congruent to 1 mod 4 is also 1 mod 4.

6.14. Let 2, p_1, p_2, $\ldots$, p_k be the first $k+1$ primes. Consider $q = 2^2 p_1 p_2 \cdots p_k - 1$. Show that $q \equiv 3 \pmod 4$, and p_i does not divide q, for $i = 1, 2, \ldots, k$.

6.15. Show that q (as above) is either a prime, or has a prime factor (different from $2, p_1, \ldots, p_k$, which is congruent to 3 mod 4.

6.16. Show that there are an infinite number of primes of the form $4n+3$.

6.17. Find the first five primes congruent to 3 mod 4.

Theorem 6.4. *Let*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \text{ and } m = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k},$$

where we allow some a_i's and b_i's to be 0. Let m_i be the minimum of a_i and b_i, and M_i the maximum of a_i and b_i, for $i = 1, 2, \ldots, k$. Then

$$(n, m) = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k};$$
$$[n, m] = p_1^{M_1} p_2^{M_2} \cdots p_k^{M_k}.$$

6.18. Prove Theorem 6.4.

Theorem 6.5. *Let n and m be two numbers. Then*

$$(n, m) \times [n, m] = nm.$$

6.19. Prove Theorem 6.5.

6.20. Let a and b be numbers with $(a, b) = 1$ and $a^3 = 25b^3$. Show that if p is a prime that divides b, then p has to divide a.

6.21. Let N, a and b be numbers with $(a, b) = 1$ and $a^m = Nb^m$ for some $m \in \mathbb{N}$. Show that $b = 1$.

6.22. Show that if N is not the mth power of a number, then $\sqrt[m]{N}$ is irrational.

6.23. List ten irrational numbers other than $\sqrt{2}$.

Remark 6.6. Let a, b and c be integers and $n \in \mathbb{N}$. The following properties indicate that the $\equiv$ relation is like the $=$ relation.

(i.) $a \equiv a \pmod{n}$.
(ii.) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
(iii.) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

Any integer is equivalent to one element of $\mathbb{Z}_n$.

Remark 6.7. Once we have a set where there is some kind of equality relation, i.e., an analogue of the '=' relation, then we can define operations on it, like addition and multiplication.

Let $a, b \in \mathbb{Z}_n$. We define addition and multiplication mod n as $a+b$ and ab, by taking the answer mod n. This defines a 'number system'. Similarly, we can take powers, solve equations, and do things we would normally do with numbers. The following properties are easy to see.

(a.) If $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$.
(b.) If $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.
(c.) If $a_1 \equiv a_2 \pmod{n}$ and c is an integer, then $ca_1 \equiv ca_2 \pmod{n}$.
(d.) If $a_1 \equiv a_2 \pmod{n}$ then $a_1^m \equiv a_2^m \pmod{n}$ for m a natural number.

These properties show that the sum and product is 'well-defined'.

6.24. Let $a \equiv b \pmod{5}$ and $a \equiv b \pmod{7}$. Show that $a \equiv b \pmod{35}$.

6.25. Let $n \mid a$ and $m \mid a$. Show that $[n, m] \mid a$. From here obtain the following. Let $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$. Show that $a \equiv b \pmod{[mn]}$.

PROBLEM SET 7

Remark. To reduce the displays of continued fractions, we write the continued fraction

$$b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \cdots}}} \text{ as } b_0 + \frac{a_1}{b_1} + \frac{a_2}{b_2} + \frac{a_3}{b_3} \cdots + \frac{a_n}{b_n} + \cdots.$$

Consider the infinite continued fraction

$$1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots.$$

In the next few problems, you are asked to compute parts of this continued fraction. If you do things cleverly, you can use the previous calculations at each step.

7.1. Write as a fraction, in the form p/q: $1 + \frac{1}{2}$.

7.2. Write as a fraction: $1 + \frac{1}{2} + \frac{1}{2}$.

7.3. Write as a fraction: $1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2}$.

7.4. Write as a fraction: $1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2}$

7.5. Show that

$$\sqrt{2} - 1 = \frac{1}{\sqrt{2}+1} = \frac{1}{2 + (\sqrt{2} - 1)}.$$

7.6. Show that:

$$\sqrt{2} = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{\sqrt{2}+1}.$$

7.7. List all the numbers $n \leq 7$ such that $(n, 7) = 1$.

7.8. List all the numbers $5n \pmod 7$, where n is in the list above in Problem 7.7.

7.9. List numbers $n \leq 10$ such that $(n, 10) = 1$.

7.10. List all the numbers $3n \pmod{10}$ where n is in the list in Problem 7.9.

7.11. Let $(k, m) = 1$. Then show that if $ka \equiv kb \pmod m$, then $a \equiv b \pmod m$.

7.12. Does $5 \mid 4!$? What is $(5, 4!)$?

7.13. Let p be a prime. Find $(p, (p-1)!)$.

7.14. Show that if $(a, p) = 1$, then the list

$$a, 2a, 3a, \ldots, (p-1)a \pmod{p}$$

is a re-ordering of $1, 2, 3, \ldots, p-1$.

7.15. Let p be a prime, and a such that $(a, p) = 1$. Show that

$$a^{p-1}(p-1)! = (p-1)! \pmod{p}.$$

7.16 (Fermat's little theorem)**.** Show that for p a prime: $a^{p-1} \equiv 1 \pmod{p}$.

Remark 7.1. We can write this as $a^p \equiv a \pmod{p}$. It is obtained by multiplying the above by a. When $a \mid p$, then both sides are 0 mod p. If not, we can cancel the a and obtain Fermat's little theorem.

Theorem 7.2. *Let $(k, m) = d$. If $ka \equiv kb \pmod{m}$, then $a \equiv b \pmod{\frac{m}{d}}$.*

7.17. Prove Theorem 7.2.

7.18. Let $(a, n) = 1$. Show there is an 'inverse of a mod n', that is, a number b such that $ab \equiv 1 \pmod{n}$.

Remark 7.3. Another set for which we can define equality and arithmetic operations is the set of polynomials. A polynomial is an expression of the form

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

where **the coefficients** a_i are some prescribed set of numbers (integers, rationals, from $\mathbb{Z}_n$). If a_n is the highest non-zero term, we say the **degree** of the polynomial is n. The x is called an **indeterminate**. Two polynomials are equal if they are of the same degree and the coefficient of x^k is the same for all k.

We use the notation $\mathbb{Q}[x]$ for the set of polynomials with rational coefficients, and similarly $\mathbb{Z}[x]$ and $\mathbb{Z}_n[x]$. We can define the arithmetic operations $+$ and $\times$ on polynomials, and also define $ap(x)$ where a is a number. The addition and multiplication is as expected by using the usual laws of arithmetic (associative, commutative, distributed), and follow the same laws of arithmetic from the set of coefficients.

7.19. Perform the required operation(s) for these polynomials in $\mathbb{Z}_3[x]$. Calculate

$$(1 + x + x^2) + (2 + x^2).$$

7.20. Multiply the following in $\mathbb{Z}_3[x]$: $(1 + 2x)(1 + x + x^2)$.

7.21. Perform the required operations over $\mathbb{Z}_3$: $(1 - x + x^2)(1 + x + x^2) + (2 + x - 2x^2)$.

7.22. Perform the required operations mod 3: $2(1 - x + 2x^2)$.

In the following problems, we compute $(1 + x)^n$ for $n = 0, 1, 2, 3, \ldots$ in the form $a_0 + a_1 x + a_2 x^2 + \cdots$, where the a_i's are numbers. At each step use the one you calculated in the previous step. Note that when $x = 1$ you get 2^n, and when $x = -1$, you get 0 (when $n > 0$). Use this to check each step.

We take: $(1 + x)^0 = 1$ and $(1 + x)^1 = 1 + x$.

7.23. Compute: $(1 + x)^2$.

7.24. Compute: $(1 + x)^3$.

7.25. Compute: $(1 + x)^4$.

PROBLEM SET 8

8.1. List numbers $n \leq 12$ such that $(n, 12) = 1$. Make the list $4 \times a \pmod{12}$, where a is in the first list. Are these lists the same? Do the same question for $5 \times a \pmod{12}$.

8.2. Let S be the set $S = \{m \in \mathbb{Z}_n \mid (m, n) = 1\}$. Let a be any member of S, i.e, $(a, n) = 1$. Then prove that the list of numbers

$$am \pmod{n}, \text{ where } m \in S,$$

is a re-ordering of the elements of S; that is, if $am_1 \equiv am_2 \pmod{n}$, then $m_1 \equiv m_2 \pmod{n}$.

Definition 8.1. We denote by $\varphi(n)$ the number of numbers $a \leq n$, such that $(a, n) = 1$. Thus $\varphi(n)$ is the number of elements in S (above). We take $\varphi(1) = 1$.

Examples 8.2. $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$.

8.3 (Fermat–Euler)**.** Let n be any number, and a such that $(a, n) = 1$. Show that

$$a^{\varphi(n)} = 1 \pmod{n}.$$

Note. Fermat is pronounced *Ferma*. Euler is pronounced *Oiler*.

Remark. To make sense of the infinite continued fraction:

$$b_0 + \frac{a_1}{b_1 + \frac{a_2}{b_2 + \frac{a_3}{b_3 \cdots + \frac{a_n}{b_n + \cdots}}}},$$

we consider the nth **convergent**, obtained by chopping off the continued fraction.

We denote the nth convergent by C_n and suppose $C_n = A_n/B_n$ written as a fraction. So, for example:

$$C_0 = b_0 = \frac{A_0}{B_0}, C_1 = b_0 + \frac{a_1}{b_1} = \frac{b_0 b_1 + a_1}{b_1} = \frac{A_1}{B_1}, C_2 = b_0 + \frac{a_1}{b_1 + \frac{a_2}{b_2}} = \frac{A_2}{B_2}.$$

The next few problems are about the continued fraction

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{1}{292 + \frac{1}{1 \cdots}}}}}.$$

8.4. For this continued fraction, compute C_0 as a fraction.

8.5. Compute C_1 as a fraction.

8.6. Compute C_2 as a fraction.

8.7. Compute C_3 as a fraction.

8.8. Do you recognize the convergents of π?

Suppose

$$(1+x)^n = \sum_{k=0}^{n} F(n,k)x^k = F(n,0) + F(n,1)x + F(n,2)x^2 + \cdots + F(n,n)x^n.$$

Show the following:

8.9. $F(n,0) = 1$, for $n = 1, 2, 3, \ldots$.

8.10. $F(n,k) = 0$, for $k = n+1, n+2, \ldots$.

8.11. $F(n,n) = 1$ for $n = 1, 2, \ldots$.

8.12. Recall that $(1+x)^4 = 1 + 4x + 6x^2 + 4x^3 + x^4$. Compute $(1+x)^5$ as follows:

$$\begin{aligned}(1+x)(1+x)^4 &= 1 + 4x + 6x^2 + 4x^3 + x^4 \\ &+ \quad x + 4x^2 + 6x^3 + 4x^4 + x^5.\end{aligned}$$

8.13. Show that:

$$F(n+1,k) = F(n,k) + F(n,k-1). \tag{8.1}$$

8.14. Use (8.1) to make a table of $F(n,k)$. This Table is called **Pascal's Triangle** even though it was known in ancient times in many civilizations, including the Indian and Chinese civilizations.

$n\backslash k$	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	1	1	0	0	0	0	0
2	1	2	1	0	0	0	0
3							
4							
5							
6							

Define $G(n,k)$ as follows: For $0 \le k \le n$:

$$G(n,k) = \frac{n!}{k!(n-k)!}.$$

For $k > n$, we define $G(n,k) = 0$.

8.15. Calculate $G(n,0)$.

8.16. Calculate $G(n,1)$, for $n = 1, 2, 3, \ldots$.

8.17. Calculate $G(n,2)$, for $n = 1, 2, 3, \ldots$.

8.18. Show that $G(n,k)$ satisfies (8.1) with F replaced by G.

8.19. Show, using induction, that $G(n,k) = F(n,k)$.

8.20. Show, using induction, that $F(n,k)$ is a natural number, provided $0 \le k \le n$.

8.21. Show that the product of n consecutive numbers is divisible by $n!$.

We now consider the sets $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{2}]$. These are 'polynomials in $\sqrt{2}$' with coefficients in $\mathbb{Q}$ and $\mathbb{Z}$. Again we can define the operations $+$ and $\times$ just like in polynomials; the only difference is that when you get $(\sqrt{2})^2$ we replace it with 2. Elements are of the form $a + b\sqrt{2}$. For example:

$$(1 - 2\sqrt{2})(1 - \sqrt{2}) = 1 + 2(\sqrt{2})^2 + \sqrt{2}(-1 - 2) = 5 - 2\sqrt{2}.$$

Definition 8.3 (Norm)**.** We define the norm as $N(a + b\sqrt{2}) := a^2 - 2b^2$.

8.22. Calculate and write in the form $a + b\sqrt{2}$: $\left(3 - 2\sqrt{2}\right) + \left(-2 - \sqrt{2}\right)$

8.23. Calculate $\left(1 + \sqrt{2}\right)\left(1 - \sqrt{2}\right)$

8.24. Calculate $N(1 + \sqrt{2})$.

8.25. Find $x \in \mathbb{Q}[\sqrt{2}]$ such that $x\left(1 + \sqrt{2}\right) = 1$.

Congratulations! You have done 200 questions so far in this course.

PROBLEM SET 9

9.1. Find $4!\mod 5$.

9.2. Find all pairs of numbers a and b in $\{1,2,3,4,5,6\}$ such that $ab \equiv 1 \pmod 7$. What is the product of the remaining numbers mod 7?

9.3. Let p be a prime. Show that if $(a,p) = 1$, then there is a b such that

$$ab \equiv 1 \pmod p.$$

Further, show that $(b,p) = 1$.

9.4. Show that if p is prime, then $(p-1)! \equiv -1 \pmod p$.

9.5. Show that if n is not a prime, then there are two non-zero numbers $k, m \in \mathbb{Z}_n$, such that $km \equiv 0 \pmod n$.

9.6. Show that if $(n-1)! \equiv -1 \pmod n$, then n has to be a prime number.

From the above we have the following theorem.

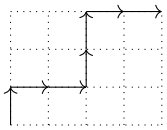
Theorem 9.1 (Wilson's theorem)**.** *Let p be a number. Then p is prime if and only if*

$$(p-1)! \equiv -1 \pmod p.$$

9.7. Recreate Pascal's triangle until $n = 8$ and expand $(x+y)^8$.

Remarks 9.2. Consider paths in the first quadrant of the Cartesian (or XY) plane beginning at $(0,0)$ and taking unit steps north and east, with a total of n steps with exactly k north steps. We are interested in counting paths.

The following is a path as above, with $n = 7$ and $k = 3$. Note that the final destination of the vertex is at $(n-k, k)$.



This path can be represented as a string of 1's and x's representing north and east steps, respectively. The string corresponding to the shown path is: $x11xx11$. This corresponds to one of the products when you multiply out

$$(1+x)(1+x)\cdots(1+x).$$

In general, each path as above corresponds to a term x^k in $(1+x)^n$. The total number of such paths will be $F(n,k)$ in our notation of PS 8. Let

$$\binom{n}{k} := \text{ the numbers of such paths.}$$

We take $\binom{0}{0} = 1$.

Note. This is called the **binomial coefficient** and read 'n choose k'. The word 'choose' comes because you are choosing k steps (from possibly n steps) to be north steps. The name binomial coefficient comes because it is the coefficient $F(n,k)$ when you expand the binomial power $(1+x)^n$.

9.8. Argue that $\binom{n}{k} = 0$ if $k > n$.

9.9. Put all paths from $(0,0)$ with n steps with exactly k north steps into two buckets: one where the last step is north, and the other where the last step is east. Using this, show that

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

9.10. Show that $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$.

9.11. List the numbers ≤ 4 that are relatively prime to 4.

9.12. List the numbers ≤ 5 that are relatively prime to 5.

9.13. List the numbers ≤ 6 that are relatively prime to 6.

9.14. List the numbers ≤ 7 that are relatively prime to 7.

9.15. List the numbers ≤ 8 that are relatively prime to 8.

9.16. List the numbers ≤ 9 that are relatively prime to 9.

9.17. Write down $\varphi(n)$ for $n = 1, \ldots, 12$.

9.18. Argue that $\varphi(p) = p - 1$, where p is a prime.

9.19. Argue that if $\varphi(n) = n - 1$, then n is a prime.

We now consider the set $\mathbb{Z}[i]$. Here i is called **iota** and is a symbol representing $\sqrt{-1}$; so $i^2 = -1$. These are 'polynomials in i' with coefficients in $\mathbb{Z}$. Again we can define the operations $+$ and $\times$ just like in polynomials; the only difference is that when you get i^2 we replace it with -1. Elements are of the form $a + ib$. These numbers are called **Gaussian Integers**.

We represent $a + ib$ by the point (a, b) in the Cartesian plane (the XY-plane).

The set $\mathbb{Z}[i]$ of Gaussian integers is a subset of the **Complex numbers** which is $\mathbb{R}[i]$; i.e., numbers of the form $x + iy$, where x and y are real numbers.

Definition 9.3 (Norm)**.** We define the norm of Gaussian integers as $N(a+bi) := a^2+b^2$.

9.20. Calculate $i^0, i^1, i^2, i^3, i^4, i^5, \ldots$. (When we say calculate in this context, we mean, write in the form $a + ib$).

9.21. Plot the points $1 = 1 + i0, 1 + i, 2i, -1 + i, -1, -1 - i, -2i, 1 - i$ on the Cartesian plane.

9.22. Calculate: $(1 + 2i)(1 - 2i)$.

Definition 9.4. The **conjugate** of a complex number/Gaussian integer $a+ib$ is defined to be $a - ib$.

9.23. Calculate: $N(1 + 2i)$. What is the distance of $1 + 2i$ from the origin?

9.24. Calculate: $(3 - 4i) + (-2 + 3i)$.

9.25. Let $z = (2 + 3i)$. Plot z, zi, zi^2 and zi^3 on the Cartesian plane. Make an arrow joining the origin to z. How do you obtain the other points from this vector?

PROBLEM SET 10

10.1. Let $(m, n) = 1$. Suppose $x = x_0, y = y_0$ is a solution of $mx - ny = 1$, then show that $x_0 + tn, y_0 + tm$ are also solutions, for all $t \in \mathbb{Z}$.

10.2. Find solutions to $3x - 13y = 1$, where both x and y are negative, and where both are positive.

10.3. Suppose $(a, n) = 1$, and $b \in \mathbb{N}$. Show that the equation $ax \equiv b \pmod{n}$ has a unique solution in $\mathbb{Z}_n$.

10.4. Suppose $(a, n) = d$, and $b \in \mathbb{N}$, and $d \mid b$. Show that the equation $ax \equiv b \pmod{n}$ has exactly d solutions in $\mathbb{Z}_n$.

10.5. Find all solutions in $\mathbb{Z}_{18}$ to the equation

$$4x \equiv 8 \pmod{18}.$$

10.6. Solve $x^2 \equiv 0 \pmod{2}$.

10.7. Solve $x^2 \equiv 1 \pmod{2}$.

The following are about the equation

$$x^2 \equiv a \pmod{p}, \tag{10.1}$$

where a is not divisible by p, so $a \not\equiv 0 \pmod{p}$.

10.8. Find all solutions to: $x^2 \equiv 1 \pmod{3}$.

10.9. Find all solutions to: $x^2 \equiv 2 \pmod{3}$.

10.10. Find all solutions to: $x^2 \equiv 3 \pmod{5}$.

10.11. Show that (10.1) can have at most two solutions.

Definition 10.1. For an odd prime p such that $p \nmid a$, we say that a is a *quadratic residue* modulo p when (10.1) has a solution in x. If (10.1) does not have a solution, we say that a is a quadratic non-residue modulo p.

10.12. Let $n < p$ Show that $(n!, p) = 1$.

10.13. Show that $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ are divisible by p.

10.14. Factor $z^3 - 1$.

10.15. Solve the equation $z^2 + z + 1 = 0$. The solution(s) are in $\mathbb{R}[i]$. You may use the quadratic formula and use $\sqrt{-d} = i\sqrt{d}$, where $d > 0$.

10.16. Let ω be one of the zeros of z^2+z+1. Show that ω^2 is also zero of this polynomial.

10.17. Find θ such that $\omega = \cos\theta + i\sin\theta$.

10.18. Draw the three roots of $z^3 - 1$ on the complex plane.

10.19. Consider $z = 1 + i$. Calculate z, ωz and $\omega^2 z$ and draw them on the plane. (You may draw a vector from the origin to z and then see what happens when it is multiplied by ω and ω^2.)

Definition 10.2. Consider the continued fraction

$$b_0 + \frac{a_1}{b_1} + \frac{a_2}{b_2} + \frac{a_3}{b_3} + \cdots.$$

The nth **convergent** written as a fraction is of the form P_n/Q_n, and is defined as:

$$\frac{P_n}{Q_n} = b_0 + \frac{a_1}{b_1} + \frac{a_2}{b_2} + \frac{a_3}{b_3} + \cdots + \frac{a_n}{b_n}.$$

We say P_n is the nth numerator, and Q_n the nth denominator. We define (for convenience) :

$$P_{-1} = 0, Q_{-1} = 1.$$

Note that

$$P_0 = b_0, Q_0 = 1.$$

10.20. Calculate P_1 and Q_1, and write them in the form

$$P_1 = b_1(*) + a_1(**) \text{ and, } Q_1 = b_1(*) + a_1(**).$$

10.21. Calculate P_2 and Q_2, and write them in the form

$$P_2 = b_2(*) + a_2(**) \text{ and } Q_2 = b_2(*) + a_2(**).$$

10.22. Calculate P_3 and Q_3 and write then in the form suggested by the above. Can you find a pattern?

10.23. Using the pattern you found, calculate P_4 and Q_4 and check if it is correct.

10.24. Calculate the first five convergents of the continued fraction

$$1 + \frac{1}{1} + \frac{1}{1} + \frac{1}{1} + \cdots.$$

10.25. Write recurrence relations for these. Can you recognize these numbers?

PROBLEM SET 11

For all problems concerning quadratic residues, **assume that p is an odd prime that does not divide a.**

Example 11.1. For any prime p, 1 is always a quadratic residue modulo p. The two solutions of $x^2 \equiv 1 \pmod{p}$ are $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{p}$.

11.1. Find all quadratic residues modulo 7. How many numbers in $\mathbb{Z}_7$ are quadratic residues and how many are quadratic non-residues.

11.2. Find all quadratic residues modulo 11. How many numbers in $\mathbb{Z}_{11}$ are quadratic residues and how many are quadratic non-residues.

11.3. Show that

$$1^2,\, 2^2,\, \ldots,\, \Big(\frac{p-1}{2}\Big)^2$$

are distinct modulo p.

11.4. How many quadratic residues modulo p are there? Non-residues?

11.5. Show that the product of two quadratic residues of p is a quadratic residue.

11.6. Let a be a quadratic residue mod p. Show that $a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$ are all distinct non-zero elements of $\mathbb{Z}_p$.

11.7. Let a be a quadratic residue mod p. Consider the set

$$S = \{am \mid m = 1, 2, \ldots, p-1\}.$$

Show that if m is a non-residue mod p, then am must be a non-residue. Thus the product of a quadratic residue of p and a quadratic non-residue of p is a quadratic non-residue of p.

11.8. Now let a be a non-residue in the set S above. Show that the product of two quadratic non-residues of p is a quadratic residue of p.

11.9. Consider the equation $3x \equiv 7 \pmod{11}$. Why do you expect the solution to be different from 3? Find the solution.

11.10. Suppose a is a quadratic non-residue of p. Show that the set $\{1, 2, \ldots, p-1\}$ can be partitioned into $\frac{1}{2}(p-1)$ pairs $\{x, x'\}$ such that $xx' \equiv a \pmod{p}$.

11.11. Show that $(p-1)! \equiv a^{\frac{1}{2}(p-1)} \pmod{p}$ if a is a non-residue mod p.

Definition 11.2 (Algebraic numbers and integers)**.** We call a complex number z an algebraic number if it is a root of an equation

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0,$$

where a_i are all integers, and $a_n \neq 0$. If $a_n = 1$, then z is said to be an **algebraic integer**.

11.12. Show that $3 + 4i$ is an algebraic integer.

11.13. Let ω be a cube root of unity, $\omega \neq 1$. Show that $7 + 3\omega$ is an algebraic integer.

11.14. Show that every element of $\mathbb{Z}[i]$ is an algebraic integer.

Definition 11.3. Today's new set where we can do arithmetic is defined as

$$\mathbb{Z}[\omega] = \{a + \omega b \mid a, b \in \mathbb{Z}\}.$$

Here ω is one of the complex cube roots of unity, say, $\omega = \frac{-1+i\sqrt{3}}{2}$. Addition and multiplication is defined, since they are complex numbers.

11.15. Show that every element of $\mathbb{Z}[\omega]$ is an algebraic integer.

11.16. Show that $7 + 3\sqrt{3}i \in \mathbb{Z}[\omega]$.

11.17. Show that $4 - 2\sqrt{3}i \in \mathbb{Z}[\omega]$.

11.18. Consider the continued fraction

$$b_0 + \frac{a_1}{b_1} + \frac{a_2}{b_2} + \frac{a_3}{b_3} + \cdots,$$

with P_n/Q_n the nth convergent. Prove, using induction, that P_n and Q_n satisfy the equations (for $n \geq 1$)

$$P_n = b_n P_{n-1} + a_n P_{n-2}, \;\; P_{-1} = 1$$

and

$$Q_n = b_n Q_{n-1} + a_n Q_{n-2}, \;\; Q_{-1} = 0$$

(Hint. For the induction step, first show that the $(n+1)$th convergent is obtained from the previous one, by replacing a_n by $a_n b_{n+1}$ and b_n by $b_n b_{n+1} + a_{n+1}$.)

Example 11.4. We give an approach to calculate $\varphi(n)$ in this example. Consider $n = 12 = 2^2 \times 3$. We want to find the number of numbers less than 12 relatively prime to 12.

- The number of numbers ≤ 12 which are divisible by 2 are $\lfloor \frac{12}{2} \rfloor = 6$.
- The number of numbers ≤ 12 which are divisible by 3 are $\lfloor \frac{12}{3} \rfloor = 4$.
- The number of numbers ≤ 12 which are divisible by *both* 2 and 3 are $\lfloor \frac{12}{6} \rfloor = 2$.
- List the numbers 1 to 12 and cross out the six divisible by 2. This leaves six numbers.
- Cross out the four numbers divisible by 3. We get $6 - 4 = 2$
- We have crossed out the ones divisible by 6 twice. So add them back again: $2 + 2 = 4$.

So the number of numbers which have no primes in common are 4. So $\varphi(12) = 4$.

11.19. Find $\varphi(18)$.

11.20. Find $\varphi(20)$.

11.21. Find $\varphi(60)$.

11.22. Find $\varphi(120)$.

11.23. Let p be a prime. Show that $\varphi(p^a) = p^a - p^{a-1}$

11.24. Let $n = p^a \times q^b$, where p and q are different primes. Show that:

$$\varphi(n) = n\Big(1 - \frac{1}{p}\Big)\Big(1 - \frac{1}{q}\Big).$$

11.25. Let $n = p_1^a \times p_2^b \times p_3^c$, where p_1, p_2, p_3 are distinct primes. Show that

$$\varphi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big)\Big(1 - \frac{1}{p_3}\Big).$$

PROBLEM SET 12

12.1. Let $n = p^a$ and $m = q^b$, where p and q are different primes. Show that

$$\varphi(nm) = \varphi(n)\varphi(m).$$

12.2. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where p_1, p_2, ..., p_k are distinct primes. Show that

$$\varphi(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_k)^{a_k}.$$

12.3. Show that if $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Definition 12.1. A number-theoretic function $f(n)$ (that is, a function that takes values on $\mathbb{N}$) is called **multiplicative** if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$.

One example of a number-theoretic function is Euler's ϕ function $\varphi(n)$. The above problem shows it is multiplicative. Another function is given by the following definition. This requires the notion of a number being **square-free**; a number is square-free if $p^2 \nmid n$, for any prime p. So $n > 1$ is square-free if it is either a prime or a product of distinct primes.

Definition 12.2 (Möbius μ-function)**.** Let p_1, p_2, ..., p_k be distinct primes. We define $\mu(1) := 1$, and, for $n > 1$,

$$\mu(n) := \begin{cases} 0, & \text{if } n \text{ is not square free;} \\ (-1)^k, & \text{if } n = p_1 p_2 \cdots p_k. \end{cases}$$

12.4. Calculate $\mu(n)$ for $n = 1, 2, 3, \ldots, 10$.

12.5. Show that $\mu(n)$ is multiplicative.

12.6. For $n = 1, 2, \ldots, 10$, compute

$$\sum_{d|n} \mu(d).$$

Here the sum is over divisors of n.

12.7. Let $n > 0$. Show that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Note that if $n = 0$, this sum is $\binom{0}{0} = 1$.

Theorem 12.3. $\displaystyle\sum_{d|n} \mu(n) = \begin{cases} 1, & \textit{if } n = 1; \\ 0, & \textit{if } n > 1. \end{cases}$

12.8. Prove Theorem 12.3. Note that if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, it is enough to consider the sum over the divisors which are square-free, so divisors which are a product of distinct primes dividing n.

12.9. Suppose b is such that $b^2 \equiv a \pmod{p}$, i.e., a is a quadratic residue modulo p. Show that the set

$$\{1, 2, \ldots, p-1\} - \{b, p-b\}$$

consisting of all numbers 1 through $p-1$, except $\pm b$, can be grouped into $\frac{1}{2}(p-3)$ pairs of distinct numbers $\{x, x'\}$ such that $xx' \equiv a \pmod{p}$.

12.10. Show that $(p-1)! \equiv -a^{\frac{1}{2}(p-1)} \pmod{p}$ if a is a quadratic residue modulo p.

Definition 12.4 (Legendre's symbol)**.** We define

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{if } a \text{ is a quadratic residue module } p\ ; \\ -1 & \text{if if } a \text{ is a quadratic non-residue module } p. \end{cases}.$$

Remark 12.5. Do not confuse this new symbol for a fraction! It takes only two integral values: -1 and 1. Note that if $a \equiv b \pmod{p}$, then we have that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Theorem 12.6. *For an odd prime p that does not divide a, we have*

$$(p-1)! \equiv -\left(\frac{a}{p}\right) a^{\frac{1}{2}(p-1)} \pmod{p}$$

12.11. Convince yourself that we have proved Theorem 12.6. Write an explanation with reference to previously done problems.

12.12. Use Theorem 12.6 to prove that $(p-1)! = -1 \pmod{p}$, for p an odd prime.

12.13. Show that $\left(\frac{-1}{p}\right)$ is congruent (and hence equal) to $(-1)^{\frac{1}{2}(p-1)}$ modulo p.

This proves the following theorem.

Theorem 12.7. *The number -1 is a quadratic residue modulo p, for all primes p of the form $4k+1$ and a quadratic non-residue modulo p, for all primes p of the form $4k+3$.*

12.14. Show that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}.$$

12.15. Show $\left(\frac{12}{37}\right) = 1$, so 12 is a residue modulo 37.

We have proved the following theorem in Problem 11.18 about computing the convergents of a continued fraction.

Theorem 12.8. *Consider the continued fraction*

$$b_0 + \frac{a_1}{b_1} + \frac{a_2}{b_2} + \frac{a_3}{b_3} + \cdots,$$

with P_n/Q_n the nth convergent. Then P_n and Q_n satisfy the recurrence relations (for $n \geq 1$)

$$P_n = b_n P_{n-1} + a_n P_{n-2}, \quad P_{-1} = 1, P_0 = b_0,$$

and

$$Q_n = b_nQ_{n-1} + a_nQ_{n-2}, \;\; Q_{-1} = 0, Q_0 = 1.$$

12.16. With the notation as in Theorem 12.8, show that

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = (-1)^{n+1}\frac{a_1a_2\dots a_n}{Q_{n-1}Q_n}. \tag{12.1}$$

12.17. Prove Cassini's (1680) identity for the Fibonacci numbers:

$$F_n^2 - F_{n-1}F_{n+1} = (-1)^{n-1}.$$

12.18. Given $a, b \in \mathbb{Z}$, write $a + b\sqrt{3}i$ as $a' + b'\omega$, where $a', b' \in \mathbb{Z}$. Hence show that $a + b\sqrt{3}i \in \mathbb{Z}[\omega]$.

We define **divisibility** and divisor in $\mathbb{Z}[i]$ in the same way as $\mathbb{Z}$.

Definition 12.9 (Divisibility in $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$)**.** An algebraic integer $z = a + bi$ is divisible by $w = m + ni$ $(\neq 0) \in \mathbb{Z}[i]$, if there exists an algebraic integer $s = c + di \in \mathbb{Z}[i]$ such that

$$a + bi = (c + di)(m + ni); \text{ i.e. } z = sw.$$

We say w is a **divisor** of z. We denote this by $w \mid z$. We define divisor similarly for $\mathbb{Z}[\omega]$.

12.19. Let s, w, z be algebraic integers. Then

$$s \mid w \text{ and } w \mid z \text{ implies } s \mid z.$$

12.20. Show that any non-zero $z \in \mathbb{Z}[i]$ is divisible by the following eight numbers:

$$1, z, -1, -z, i, iz, -i, -iz.$$

These are called the **trivial divisors**.

12.21. For $z \in \mathbb{Z}[\omega]$, what should the trivial divisors be?

Definition 12.10. A **unit** in $\mathbb{Z}[i]$ is an algebraic integer that divides every element in $\mathbb{Z}[i]$.

12.22. Show that ε is a unit if and only if it is a divisor of 1.

12.23. Show that i^k, where $k = 0, 1, 2, 3$ are all the units of $\mathbb{Z}[i]$.

12.24. Show that $(-\omega)^k$, where $k = 0, 1, 2, 3, 4, 5$ are all the units of $\mathbb{Z}[\omega]$.

12.25. Let $z_1 = 3 + 4i$ and $z_2 = -4 + 3i$. Show that $z_1 \mid z_2$ and $z_2 \mid z_1$. Let ε be such that $z_1 = \varepsilon z_2$. Show that ε is a unit.

PROBLEM SET 13

13.1. Find all solutions of $7x \equiv 1 \pmod 5$, and $5y \equiv 1 \pmod 7$. Suppose the solutions are $x = a + 5t_1$ and $y = b + 7t_2$ respectively. Use these solutions to find x_0 and y_0 such that $7x_0 + 5y_0 = 1$.

13.2. Find x and y such that $7x + 12y = 1$ using this technique.

13.3. Let $(m, n) = 1$. Let x and y be integers such that $mx+ny = 1$. Let $X = mxb+nya$. Show that

$$X \equiv a \pmod m \text{ and } X \equiv b \pmod n.$$

Let $S_n = \sum_{d|n} \varphi(d)$.

13.4. Calculate S_n for $n = 1, 2, \ldots, 10$.

13.5. Let $n = p^a$, where p is a prime. Show that $S_n = n$.

13.6. Let $n = p^a q^b$, where p and q are distinct primes. Show that $S_n = n$.

13.7. Write down the coefficient of x^0, x^1, x^2 in the expansion of

$$(1 + a_1x)(1 + a_2x)$$

as a polynomial.

13.8. Write down the coefficient of x^0, x^1, $\ldots$, x^3 in the polynomial expansion of

$$(1 + a_1x)(1 + a_2x)(1 + a_3x).$$

13.9. Write down the coefficient of x^0, x^1, $\ldots$, x^4 in the expansion of

$$(1 + a_1x)(1 + a_2x)(1 + a_3x)(1 + a_4x).$$

The above expressions in a_i are called **elementary symmetric polynomials** of $a_1, a_2, \ldots, a_n$, where n is the degree of the polynomial

Definition 13.1 (Elementary symmetric polynomial)**.** The elementary symmetric polynomial of degree k in a_1, a_2, $\ldots$, a_n, denoted e_k, is the coefficient of x^k in

$$\prod_{i=1}^{n}(1 + a_ix) = (1 + a_1x)(1 + a_2x)\cdots(1 + a_nx).$$

You have seen the usefulness of calculating such functions in computing $\varphi(n)$.

Theorem 13.2. *Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where p_1, p_2, ..., p_k are distinct primes. Then*

$$\varphi(n) = n \prod_{i=1}^{k} \Big(1 - \frac{1}{p_i}\Big). \tag{13.1}$$

Note. Theorem 13.2 should have been proved first before you proved $\varphi(n)$ is a multiplicative function.

13.10. Let n be as above. Show that

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Verify this for $n = 3, 10$.

13.11. Show that if $z_1, z_2 \in \mathbb{Z}[i]$, and $z_1 \mid z_2$ and $z_2 \mid z_1$, then $z_1 = \varepsilon z_2$, where ε is a unit.

13.12. Let $z_1, z_2 \in \mathbb{Z}[\omega]$. Show that if $z_1 \mid z_2$ and $z_2 \mid z_1$, then $z_1 = \varepsilon z_2$, where ε is a unit.

13.13. For $z = a + ib \in \mathbb{Z}[i]$, recall the **norm** $N(z) = a^2 + b^2$, and the complex conjugate $\overline{z} = a - ib$ of z. We denote by $|z|$ the distance of z from the origin. Show that

$$N(z) = z\overline{z} = |z|^2.$$

13.14. Let $a, b, c, d \in \mathbb{Z}$, Show that

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ad - bc)^2.$$

13.15. Let $z, w \in \mathbb{Z}[i]$. Show that

$$N(z)N(w) = N(zw).$$

13.16. Show that $\varepsilon \in \mathbb{Z}[i]$ is a unit if and only if $N(\varepsilon) = 1$.

Definition 13.3. If ε is a unit, then εz is said to an **associate** of z.

13.17. What are the associates of z in $\mathbb{Z}[i]$?

Remark 13.4. The associates of any non-zero algebraic integer are a subset of its trivial divisors.

13.18. If z divides w, then show that any associate of z divides any associate of w.

Definition 13.5. A algebraic integer π is a prime if it is not 0 and not a unit, divisible only by numbers associated with itself or with 1. In other words, the only divisors of a prime are all the trivial divisors.

Theorem 13.6. *If z is an algebraic integer such that $N(z) = p$, where $p \in \mathbb{Z}$ is prime, then z is a prime in $\mathbb{Z}[i]$.*

13.19. Prove Theorem 13.6.

13.20. Show that 3 is a prime in $\mathbb{Z}[i]$ and $N(3) = 9$.

13.21. Show that the converse of Theorem 13.6 is not true.

13.22. What is $N(2+i)$. Does this give enough evidence to say that $2+i$ is a prime in $\mathbb{Z}[i]$?

13.23. Show that 5 is not a prime in $\mathbb{Z}[i]$.

13.24. What are the divisors of 15 in $\mathbb{Z}[i]$?

Remark 13.7. When performing the GCD algorithm with $n = q_0m+r_0$, $m = q_1r_0+r_1$, $r_0 = q_2r_1 + r_2$, ..., we obtain a continued fraction where $a_i = 1$, for all i.

We obtain the continued fraction

$$b_0 + \frac{1}{b_1} + \frac{1}{b_2} + \frac{1}{b_3} + \cdots + \frac{1}{b_n},$$

with $b_i > 0$, for $i = 1, 2, \ldots, n$, for some n. As earlier, let P_n/Q_n denote the nth convergent. Theorem 12.8 shows that P_n and Q_n satisfy the recurrence relations (for $n \geq 1$)

$$P_n = b_nP_{n-1} + P_{n-2}, \quad P_{-1} = 1, P_0 = b_0$$

and

$$Q_n = b_nQ_{n-1} + Q_{n-2}, \quad Q_{-1} = 0, Q_0 = 1.$$

With this notation, Problem 12.16 can be written as

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n+1}. \tag{13.2}$$

From now on we consider this continued fraction, with $a_i = 1$ and $b_i > 0$.

13.25. With the notation as above, show that

$$P_nQ_{n-2} - P_{n-2}Q_n = (-1)^n b_n. \tag{13.3}$$

PROBLEM SET 14

14.1. Let $n = p^a$, where p is a prime. Find all the factors of n. How many are there?

14.2. Let $n = p^a q^b$, where p and q are distinct primes. Find all the factors of n. How many are they?

14.3. Let $n = 3^3 5^2$. Verify that

$$\Big(1 + \varphi(3) + \varphi(3^2) + \varphi(3^3)\Big)\Big(1 + \varphi(5) + \varphi(5^2)\Big) = \sum_{d|n} \varphi(d).$$

14.4. Let $n = p_1^{a_1} \cdots p_k^{a_k}$ Show that

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} \Big(1 + \varphi(p_i) + \varphi(p_i^2) + \cdots + \varphi(p_i^{a_i})\Big).$$

Theorem 14.1. *Let n be a natural number.*

$$\sum_{d|n} \varphi(d) = n.$$

14.5. Prove Theorem 14.1.

14.6. Let $n = 23$ and $m = 8$. Find integers q and r such that $n = mq + r$, where $0 < r < m$.

14.7. Let $n = 23$ and $m = 8$. Find integers q and r such that $n = mq + r$, where $-\frac{m}{2} < r \leq \frac{m}{2}$.

14.8. Let $n = -23$ and $m = 8$. Find integers q and r such that $n = mq + r$, where $0 < r < m$.

14.9. Let n and m be numbers. Show there are integers q and r such that $n = mq + r$, where $-\frac{m}{2} < r \leq \frac{m}{2}$.

Note. Let n be a number. Any number m has a remainder in $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. We can also find a remainder in the set

$$\Big\{ -\Big\lfloor \frac{n}{2} \Big\rfloor + 1, \ldots, \Big\lfloor \frac{n}{2} \Big\rfloor \Big\}.$$

All we want in this context is that the remainder r is such that the absolute value of r is the smallest possible. This is what the problem above is about.

14.10. Consider the equation

$$a^2 + b^2 = c^2. \tag{14.1}$$

Show that $(n+1)^2 - n^2 = 2n + 1$. Write this equation for $n = 1, 2, 3, 4, 5, \ldots$ until you find two solutions to Equation 14.1 in natural numbers. Show that there are an infinite number of solutions to this equation with a, b and c natural numbers.

Definition 14.2. The triple (a, b, c) of numbers is called a Pythagorean triplet if $a^2 + b^2 = c^2$.

14.11. Find all solutions of (14.1) when $a = 0$ or $a = 1$.

14.12. Let $z = x + iy$ such that $z \times \overline{z} = 1$. What is the distance of z from the origin? Write $z \times \overline{z} = 1$ in terms of x and y.

14.13. Let (x, y) be a point in the first quadrant on the unit circle, i.e., the circle with center at the origin and radius 1. Draw the line segment joining the points $(-1, 0)$ and (x, y). (Make a picture). Let $(0, m)$ be the point where this line segment crosses the y-axis. Find the equation of the line containing this line segment. What is the slope of this line?

14.14. The point (x, y) lies on this line as well as the circle with equation $x^2 + y^2 = 1$. Use this fact to prove

$$(1 + m^2)x^2 + 2m^2x + m^2 - 1 = 0.$$

14.15. Show that

$$x = \frac{1 - m^2}{1 + m^2} \text{ and } y = \frac{2m}{1 + m^2}.$$

14.16. Suppose m is a positive rational number, between 0 and 1, of the form $m = p/q$, with p and q integers. Use the above to find an infinite set of solutions to (14.1).

14.17. Argue that any solution of (14.1) with $a, b, c > 0$ has to correspond to a rational number m between 0 and 1. Thus all Pythagorean triples are obtained in this manner.

Note. The above outlines an approach to find all Pythagorean triples (a, b, c), when a, b, c are natural numbers.

14.18. Show that for any $\gamma \in \mathbb{Z}[i]$ that is neither 0 nor a unit, then either γ is a prime or there exists $\alpha \in \mathbb{Z}[i]$ such that $\alpha \mid \gamma$ and $N(\alpha) < N(\gamma)$.

14.19. Use WOP to show that if $\gamma \in \mathbb{Z}[i]$ is neither 0 nor a unit, then there exists a prime $\pi \in \mathbb{Z}[i]$ such that $\pi \mid \gamma$.

Theorem 14.3. *If $\gamma \in \mathbb{Z}[i]$ is neither 0 nor a unit, then γ can be written as a product of primes in $\mathbb{Z}[i]$.*

14.20. Prove Theorem 14.3, using induction on norm of γ.

14.21. Let $\gamma = 5 + 4i$ and $\delta = 3 + i$.

(a.) Calculate $z = \gamma/\delta = x + iy$, where x, y are rational numbers.
(b.) Find integers a, b such that $|x - a| \leq \frac{1}{2}, |y - b| \leq \frac{1}{2}$. (Make a picture!)
(c.) Calculate $r = \gamma - (a + ib)\delta$, where a, b are the integers as in the previous part.

(d.) Verify that $N(r) \leq \frac{1}{2}N(\delta)$.

14.22. Let $\gamma = 7 + 3i$ and $\delta = 3 + i$.

(a.) Calculate $z = \gamma/\delta = x + iy$, where x, y are rational numbers.
(b.) Find integers a, b such that $|x - a| \leq \frac{1}{2}, |y - b| \leq \frac{1}{2}$.
(c.) Calculate $r = \gamma - (a + ib)\delta$, where a, b are the integers as in the previous part.
(d.) Verify that $N(r) \leq \frac{1}{2}N(\delta)$.

14.23. Let $\gamma = 5 + 4i$ and $\delta = 2 + 3i$.

(a.) Calculate $z = \gamma/\delta = x + iy$, where x, y are rational numbers.
(b.) Find integers a, b such that $|x - a| \leq \frac{1}{2}, |y - b| \leq \frac{1}{2}$.
(c.) Calculate $r = \gamma - (a + ib)\delta$, where a, b are the integers as in the previous part.
(d.) Verify that $N(r) \leq \frac{1}{2}N(\delta)$.

Theorem 14.4 (Euclid's division lemma for Gaussian integers)**.** *Given $\gamma, \delta \in \mathbb{Z}[i]$, such that $\delta \neq 0$, then there exists $q, r \in \mathbb{Z}[i]$ such that*

$$\gamma = \delta q + r, \text{ such that } N(r) < N(\delta).$$

14.24. Prove Theorem 14.4.

14.25. Show that a stricter inequality: $N(r) \leq \frac{1}{2}N(\delta)$ holds, in the statement of Theorem 14.4.

PROBLEM SET 15

15.1. Let $(m, n) = 1$. Let $X \in \mathbb{Z}_n$ and $Y \in \mathbb{Z}_m$ be solutions of

$$mx \equiv 1 \pmod{n} \tag{15.1}$$

$$ny \equiv 1 \pmod{m}. \tag{15.2}$$

Then all solutions of (15.1) are given by $X + nt_1$, where t_1 are integers. Similarly, solutions of (15.2) are $Y + mt_2$, for integers t_2. Let $T = t_1 + t_2$. Show that the equation in T given by

$$mX + nY + mnT = 1$$

has an integral solution. From here, taking $t_1 = 1$, $t_2 = T - 1$ we obtain $x = X + t_1$ and $y = Y + t_2$ such that $mx + ny = 1$.

Remark 15.1. This gives a constructive approach to computing x and y such that $mx + ny = 1$, when $(m, n) = 1$. It is easy to do this for all examples. How will you apply this approach when $(m, n) = d$?

15.2. Find x and y such that $12x + 15y = 3$.

For the next few problems, consider the continued fraction

$$b_0 + \frac{1}{b_1} + \frac{1}{b_2} + \frac{1}{b_3} + \cdots,$$

with $b_i > 0$, for $i = 1, 2, \ldots, n$, for some n. Such a continued fraction is called a **simple** continued fraction. As earlier, let P_n/Q_n denote the nth convergent. We have proved the following relations:

$$P_n = b_n P_{n-1} + P_{n-2}, \quad P_{-1} = 1, P_0 = b_0, \tag{15.3a}$$

$$Q_n = b_n Q_{n-1} + Q_{n-2}, \quad Q_{-1} = 0, Q_0 = 1. \tag{15.3b}$$

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n+1}; \tag{15.3c}$$

$$P_n Q_{n-2} - P_{n-2} Q_n = (-1)^n b_n. \tag{15.3d}$$

15.3. As above, let $b_i > 0$ for all i. Show that the even convergents P_{2n}/Q_{2n} increase strictly with n; that is

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \cdots.$$

15.4. Show that the odd convergents P_{2n-1}/Q_{2n-1} decrease strictly with n; that is

$$\frac{P_1}{Q_1} > \frac{P_3}{Q_3} > \frac{P_5}{Q_5} > \cdots.$$

15.5. Argue that $Q_{n+1} > Q_n$ (for $n > 1$); that is, the size of the denominators of the convergents keeps increasing.

15.6. Show that $(P_n, Q_n) = 1$.

15.7. Show that:

$$\frac{P_{2n+1}}{Q_{2n+1}} - \frac{P_{2n}}{Q_{2n}} = \frac{1}{Q_{2n+1}Q_{2n}} < \frac{1}{Q_{2n}^2}.$$

This shows that as n increases, the difference between the convergents becomes smaller and smaller.

Remark 15.2. The above properties show that the convergents of a continued fraction where $a_i = 1$ and $b_i > 0$ (for all i) **converge** to a real number. Conversely, we can copy the Euclidean algorithm to find the continued fraction of any real number.

15.8. Consider the infinite continued fraction

$$w = 1 + \frac{1}{1} + \frac{1}{1} + \cdots.$$

Assume the continued fraction converges to a positive real number. Show that

$$w = \frac{1+\sqrt{5}}{2}.$$

The decimal expansion of this number is $1.61803398874989484820458 7\ldots$

15.9. Suppose

$$x = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} \cdots$$

converges and is positive. Find the value of x.

15.10. Show that a rational number of the form p/q cannot have an infinite simple continued fraction.

15.11. Prove that $(1 + \sqrt{5})/2$ is irrational. Use this to prove $\sqrt{5}$ is irrational.

15.12. Use a calculator to compute the first few terms for the continued fraction of π, which is a real number with the decimal expansion that begins:

$$\begin{aligned}\pi =& 3.14159265358979323846264338327\\ & 95028841971693993751058209749 44\\ & 59230781640628620899862803482 53\ldots\end{aligned}$$

You need to only take the first eight digits in your computations.

Definition 15.3. A **complete set of residues** mod n is a set of numbers $r_1, r_2, \ldots, r_n$ such that $r_i \equiv i \pmod{n}$, for $i = 1, 2, 3, \ldots, n$.

Remark 15.4. The set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ forms a complete set of residues modulo n. Another set we use is

$$\Big\{ -\Big\lfloor \frac{n}{2} \Big\rfloor + 1, \ldots, \Big\lfloor \frac{n}{2} \Big\rfloor \Big\}.$$

Here we take r_i such that $-\frac{n}{2} < r_i \leq \frac{n}{2}$. List this set for $n = 3, 4$ to understand what it is.

15.13. Consider the list of numbers

$$1 \cdot 3, 2 \cdot 3, 3 \cdot 3, 4 \cdot 3, 5 \cdot 3.$$

Consider them mod 11, and find corresponding residues between $-\frac{11}{2}$ and $\frac{11}{2}$.

15.14. Suppose p does not divide m. Show that each of the numbers

$$1m, 2m, \ldots, \frac{1}{2}(p-1)m,$$

is congruent to exactly one number modulo p between $-\frac{p}{2}$ and $\frac{p}{2}$.

Definition 15.5. The minimal residue of a modulo p is a number r such that

$$r \equiv a \pmod{p}, \text{ with } r \text{ such that } -\frac{p}{2} < r < \frac{p}{2}.$$

15.15. Suppose p does not divide m. Show that we can write the minimal residues modulo p of

$$1m, 2m, \ldots, \frac{1}{2}(p-1)m$$

in the form

$$r_1, \ldots, r_\lambda, -s_1, \ldots, -s_\mu$$

where $\lambda + \mu = \frac{1}{2}(p-1)$, $0 < r_i < \frac{p}{2}$ and $0 < s_i < \frac{p}{2}$.

15.16. Show that in Problem 15.15, the numbers $r_1, \ldots, r_\lambda$ are distinct.

15.17. Show that in Problem 15.15, the numbers $s_1, \ldots, s_\mu$ are distinct.

15.18. Show that in Problem 15.15, $r_i \neq s_j$ for all i and j; that is, no r_i is equal to any s_j.

Remark. We have shown that

$$r_1, \ldots, r_\lambda, s_1, \ldots, s_\mu$$

is a rearrangement of the numbers

$$1, 2, \ldots, \frac{p-1}{2}.$$

15.19. Let p be a prime that does not divide m. Show that

$$m^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod{p}.$$

Theorem 15.6 (Gauss Lemma)**.** *Let p be a prime, and m such that p does not divide m. Then the Legendre symbol*

$$\left(\frac{m}{p}\right) = (-1)^\mu,$$

where μ is the number of members of the list

$$m, 2m, \ldots, \frac{1}{2}(p-1)m$$

whose minimal residue modulo p is less than 0.

15.20. Prove Theorem 15.6.

Remark 15.7. In the context of the Gaussian integers, we have proved the division lemma in Theorem 14.4. We can apply the division algorithm repeatedly to obtain the GCD of two Gaussian integers α and β. In the following problems, make calculations analogous to those with natural numbers to obtain the GCD of two Gaussian integers, where division is done like in Problem Set 14.

15.21. Find $(6+7i, 11+3i)$ in $\mathbb{Z}[i]$. (Here (α, β) denotes the GCD of α and β. Sometimes we use $\mathrm{GCD}(\alpha, \beta)$.)

15.22. Find $(4+3i, 12+5i)$ in $\mathbb{Z}[i]$.

We have reordered somewhat and made changes to PS 15.

Theorem 15.8. *Let α, β be non-zero elements of $\mathbb{Z}[i]$. Show there is an element $\delta \in \mathbb{Z}[i]$ such that:*

(i.) $\delta \mid \alpha$ *and* $\delta \mid \beta$.
(ii.) If $\delta_1 \mid \alpha$ *and* $\delta_1 \mid \beta$, *then* $\delta_1 \mid \delta$.

Definition 15.9. This δ is called the greatest common divisor of α and β, and it is determined upto a unit; i.e., if δ is the GCD, then $\varepsilon\delta$ also satisfies above conditions, for all units ε in $\mathbb{Z}[i]$.

15.23. Prove Theorem 15.8. To do so, consider the set S:

$$S = \big\{N(\alpha x + \beta y) \mid x, y \in \mathbb{Z}[i]\big\}.$$

Show using WOP this has a least element d and there is a δ such that $N(\delta) = d$, $\delta = \alpha x + \beta y$ for some x, y, and δ satisfies the required properties.

15.24. Let $\pi, \gamma, \mu \in \mathbb{Z}[i]$ be such that π is a prime. Suppose $(\pi, \gamma) = \mu$. Show that either

(i.) μ is a unit and $(\pi, \gamma) = 1$; or,
(ii.) $\pi \mid \gamma$ and μ is an associate of π.

Theorem 15.10. *Let $\pi, \alpha, \beta \in \mathbb{Z}[i]$. Let π be a prime. If $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$.*

15.25. Prove Theorem 15.10. More generally, prove the following. Let $\gamma, \alpha, \beta \in \mathbb{Z}[i]$ such that $\mathrm{GCD}(\alpha, \beta) = 1$. Show that if $\alpha \mid \beta\gamma$, then $\alpha \mid \gamma$.

Bonus. What is 15×25? This is the number of problems you have done so far in this course!

PROBLEM SET 16

16.1. Show that

$$1 \cdot 2 + 2 \cdot 5 + \cdots + n(3n-1) = n^2(n+1).$$

16.2. Prove that if p is a prime, then every prime divisor of $2^p - 1$ is greater than p and congruent to 1 mod p.

Note. We say m and n are **co-prime**, or **relatively prime**, if $(m, n) = 1$.

16.3. Show that $(n, n+1) = 1$, that is, two successive numbers are relatively prime.

16.4. Find x and y such that $15x+24y = 3$ by first finding x and y such that $5x+4y = 1$.

16.5. Suppose x_1 and x_2 satisfy $nx_1 \equiv 1 \pmod{m}$ and $mx_2 \equiv 1 \pmod{n}$. Show that $X = anx_1 + bmx_2$ is a solution of the system

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

Moreover, if y is another solution, then

$$y \equiv x \pmod{mn}.$$

16.6. Prove using induction that if $X = Y \pmod{m_i}$ for $i = 1, \ldots, k$, and m_i are pairwise co-prime, then $X = Y \pmod{M}$, where $M = m_1 m_2 \cdots m_k$. The $k = 2$ case is Problem 6.25.

16.7. Find a solution to each equation: $5x_1 \equiv 1 \pmod{11}$, $11x_2 \equiv 1 \pmod{5}$. Use your answers to find a solution for the system:

$$x = 7 \pmod{11}$$
$$x = 2 \pmod{5}$$

16.8. Show that your solution to the problem above is unique modulo 55; i.e., if y is another solution, then $y \equiv x \pmod{55}$.

16.9. Find a solution to each equation: $35x_1 \equiv 1 \pmod{11}$, $55x_2 \equiv 1 \pmod{7}$, and, $77x_2 \equiv 1 \pmod{5}$. Use your answers to find a solution for the system:

$$x = 8 \pmod{11}$$
$$x = 3 \pmod{7}$$
$$x = 4 \pmod{5}$$

16.10 (Sun Tzu)**.** Find a number which leaves the remainders 2, 3 and 2 when divided by 3, 5 and 7, respectively.

Remark 16.1 (Chinese remainder theorem)**.** The above problems are about solving a system of equations of the form

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

where $m_1, m_2, \ldots, m_k$ are pairwise co-prime (have GCD 1).

The technique to solve it is as follows: Let $M = m_1 m_2 \cdots m_k$, and $M_i = M/m_i$.

Step 1: Find x_1, x_2, ..., x_m such that $M_i x_i \equiv \pmod{m_i}$, for $i = 1, 2, \ldots, k$. In other words, find the inverse mod m_i for M_i.

Step 2: The solution is given by

$$X = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_k M_k x_k.$$

The solution is unique modulo M (by Problem 16.6).

16.11. Prove that in Problem 15.1, if we find the solutions x and y such that $x \in \mathbb{Z}_n$ and $y \in \mathbb{Z}_m$, we will always obtain $t_1 + t_2 = -1$.

Theorem 16.2 (Fundamental Theorem of Arithmetic in $\mathbb{Z}[i]$)**.** *A Gaussian integer can be expressed in only one way as a product of primes in standard form upto units; that is, apart from reordering the primes, there is only one way of expressing a number as a product of primes.*

16.12. Show that any number $\zeta \in \mathbb{Z}[i]$ can be written in the form $\zeta = \varepsilon \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k}$, where $\pi_1, \pi_2, \ldots, \pi_k$ are the primes dividing ζ, $a_i > 0$ and ε is a unit in $\mathbb{Z}[i]$.

16.13. Suppose $\zeta = \varepsilon \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k}$, and $\zeta = \varepsilon' \rho_1^{b_1} \rho_2^{b_2} \cdots \rho_l^{b_l}$, where the π_i's and ρ_i's are primes in $\mathbb{Z}[i]$ and a_i's and b_i's natural numbers and $\varepsilon, \varepsilon'$ are units in $\mathbb{Z}[i]$. Here π_i's are distinct and ρ_i's are distinct. Show that π_1 is associate to ρ_j for some j.

16.14. Suppose $\zeta = \varepsilon \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k}$, and $\zeta = \varepsilon' \pi_1^{b_1} \pi_2^{b_2} \cdots \pi_k^{b_k}$, where the π_i's are distinct primes and $\varepsilon, \varepsilon'$ are units in $\mathbb{Z}[i]$. Show that $a_1 = b_1$.

16.15. Use the above to complete the proof of Theorem 16.2.

Remark 16.3. In both $\mathbb{Z}$ and $\mathbb{Z}[i]$, the fundamental theorem of arithmetic asserts that every non-zero, non-unit element in these sets can be factorized uniquely into primes, disregarding the order of the primes. This property is known as the **unique factorization property**. However, it is important to note that not all number systems possess this property.

16.16. Look at all the steps in the proof of the fundamental theorem of arithmetic for $\mathbb{Z}$ and for $\mathbb{Z}[i]$. Which step in each proof uses Euclid's division algorithm?

16.17. Let $\zeta \in \mathbb{Z}[i]$ such that $N(\zeta) = p^k$ for some positive integer k and prime p. Show that ζ is a product of at most k primes upto units.

Definition 16.4 (Greatest integer function)**.** For x a real number, we define $\lfloor x \rfloor$ as the greatest integer not exceeding x. For example, $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$. For any integer n, we have that $\lfloor n \rfloor = n$

Gauss's lemma can be used to determine whether a certain number is a quadratic residue for any odd prime p. We answer the question: when is 2 a quadratic residue modulo p? In other words, we are computing the Legendre symbol $\left(\frac{m}{p}\right)$ for $m = 2$.

In the following, consider the list of numbers mod p.

$$1 \cdot m, 2 \cdot m, \ldots, \frac{p-1}{2} \cdot m.$$

We take $m = 2$ in the following, so consider the list.

$$2, 4, \ldots, p-1. \tag{16.1}$$

In this case λ is the number of numbers in this list which are $< p/2$ and μ is the number of numbers $> p/2$ (Why?).

16.18. Suppose $p = 8k+1$. How many numbers in the list (16.1) are between 0 and $p/2$? How many are between $p/2$ and p? Argue that $\lambda = 2k$ and $\mu = 2k$.

16.19. Suppose $p = 8k+3$. Show that $\lambda = 2k$ and $\mu = 2k+1$.

16.20. Suppose $p = 8k+5$. Show that $\lambda = 2k+1$ and $\mu = 2k+1$.

16.21. Suppose $p = 8k+7$. Show that $\lambda = 2k+1$ and $\mu = 2k+2$.

16.22. Show that

$$\left\lfloor \frac{p+1}{4} \right\rfloor = \mu,$$

for each of the cases $p = 8k+1, 8k+3, 8k+5$ and $8k+7$.

Theorem 16.5. *Let p be an odd prime. Then the Legendre symbol $\left(\frac{2}{p}\right)$ is given by:*

$$\left(\frac{2}{p}\right) = (-1)^{\left\lfloor \frac{p+1}{4} \right\rfloor};$$

that is, 2 is a quadratic residue of primes of the form $8n \pm 1$ and a quadratic non-residue for primes of the form $8n \pm 3$.

16.23. Prove Theorem 16.5.

16.24. Calculate $\left(\frac{2}{p}\right)$ for $p = 17, 19, 29, 31$.

16.25 (Bhaskara)**.** A basket contains n mangoes. If they are distributed among 2 people, one mango is left. If we distribute among $3, 5$ or 7 people, we are left with $2, 4$ or 6 mangoes, respectively. However we can distribute equally among 11 people. Find the smallest such n.

PROBLEM SET 17

17.1. Show that

$$1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(4n^2-1)}{3}.$$

17.2. Let f_n denote the Fibonacci numbers. Show that $(f_n, f_{n+1}) = 1$ for $n \geq 1$.

17.3. List the Fibonacci numbers until f_{10}. Find n such that $(f_8, f_{10}) = f_n$.

17.4. Find n such that $(f_6, f_9) = f_n$.

Remark 17.1 (Algorithm to find the GCD-I)**.** Consider the sequence of steps to find the GCD of n and m. Suppose quotients q_i and remainders r_i are obtained at each step. Suppose $r_{n+1} = 0$, the the rest of the $r_i's$ satisfy

$$\begin{aligned} n &= mq_1 + r_1 \\ m &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n+1} \end{aligned}$$

17.5. Let $d = (m, n)$. Show that $d \mid r_n$.

17.6. Let $d = (n, m)$ and d' be any other common divisor of d. Show that $d' \mid d$.

17.7. Let $d = (m, n)$. Show that $r_n \mid d$.

Remark 17.2. This shows $d = r_n$.

17.8. Show that $\frac{1}{8}(p^2 - 1)$ is even for a prime of the form $p = 8k \pm 1$.

17.9. Show that $\frac{1}{8}(p^2 - 1)$ is odd for a prime of the form $p = 8k \pm 5$.

Remark 17.3. This shows that for odd primes p:

$$\left\lfloor \frac{p+1}{4} \right\rfloor = \left\lfloor \frac{p^2-1}{8} \right\rfloor \pmod 2.$$

So Theorem 16.5 can be written as follows. For p an odd prime,

$$\left(\frac{2}{p}\right) = (-1)^{\left\lfloor \frac{p+1}{4} \right\rfloor} = (-1)^{\left\lfloor \frac{p^2-1}{8} \right\rfloor}.$$

17.10. Calculate $\left(\frac{2}{3}\right)$

17.11. Calculate $\left(\frac{2}{5}\right)$.

17.12. Calculate $\left(\frac{2}{7}\right)$.

17.13. Calculate $\left(\frac{2}{11}\right)$.

Theorem 17.4 (Quadratic Reciprocity Law (Gauss))**.** *For distinct odd primes p and q, we have that*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Note. We will outline the proof in later problem sets. For now, learn to calculate using Gauss' quadratic reciprocity law.

17.14. Show that if $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

17.15. Show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

17.16. Show that $\left(\frac{a^2}{p}\right) = 1$.

17.17. Calculate $\left(\frac{11}{13}\right)$.

17.18. Calculate $\left(\frac{13}{23}\right)$.

17.19. Calculate $\left(\frac{39}{31}\right)$.

17.20. Calculate $\left(\frac{91}{23}\right)$.

Theorem 17.5 (Fermat's theorem on sums of two squares)**.** *Let p be an odd prime p. Then if $p \equiv 1 \pmod{4}$ it can be written as a sum of two squares of integers. Conversely, if $p = x^2 + y^2$ for some numbers x and y, then $p \equiv 1 \pmod{4}$.*

The next few problems give an outline of the proof.

17.21. Let $p \in \mathbb{Z}$ is a prime such that $p \equiv 1 \pmod{4}$. Show that there exists $m \in \mathbb{Z}$ such that $p \mid (m^2 + 1)$.

17.22. Let p, m be as above, with $p \mid m^2 + 1$. Then show that $p \nmid m + i$ and $p \nmid m - i$. Conclude from this that p is not a prime in $\mathbb{Z}[i]$.

17.23. Use Theorem 16.2, along with the fact that $N(p) = p^2$ to conclude that $p = (x + iy)(x - iy)$, where $x + iy$ and $x - iy$ are primes in $\mathbb{Z}[i]$.

17.24. Let $p \in \mathbb{Z}$ is a prime such that $p \equiv 3 \pmod{4}$. Show that there is no solution (x, y) such that $x^2 + y^2 = p$ in integers. (Hint: Look at the equation mod 4.)

Remark 17.6. Convince yourself that you have proved Theorem 17.5.

17.25 (The monkey and the coconuts (Williams (1926))). Five men and a monkey were shipwrecked on an island. They spent the first day gathering coconuts for food.

During the night, one man woke up, and decided to take his share early. So he divided the coconuts in five piles. He had one coconut left over, and he gave that to the monkey. Then he hid his pile and put the rest back together.

By and by each of the five men woke up and did the same thing, one after the other: each one taking a fifth of the coconuts that were in the pile when he woke up, and having one left over for the monkey. In the morning they divided what coconuts were left, and they came out in five equal shares. Of course each one must have known there were coconuts missing; but each one was guilty as the others, so they didn't say anything.

How many coconuts were there in the original pile?

Note. Suppose you are allowed a negative number of coconuts, and each person gives one to the monkey *before* dividing the coconuts (to get -5 coconuts to divide by 5) and taking their share (which is -1). Convince yourself that -4 coconuts is a solution to this puzzle!

Remark 17.7. You have seen elements of the arithmetic in $\mathbb{Z}[i]$, and $\mathbb{Z}[\omega]$, where ω is the cube root of unity. We have seen that Euclid's division lemma works in $\mathbb{Z}[i]$, and this led to a unique factorization theorem. In fact, this works even in $\mathbb{Z}[\omega]$. However, not all such sets have a unique factorization.

For example, consider

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\},$$

with $N(a + b\sqrt{-5}) = a^2 + 5b^2$ as the norm. We can define arithmetic in this set too. But both 3 and $2 + \sqrt{-5}$ have norm 9, indicating that they both divide 9 ($9 = 3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5})$). We can show these elements cannot be written as a product of two non-units. They are called **irreducible elements**. Further, we can show that 3 does not share any common factors with $(2 \pm \sqrt{-5})$. Thus unique factorization does not hold here.

The subject of **Algebraic Number Theory** considers these number systems and their properties.

PROBLEM SET 18

18.1. Calculate $\left(\frac{2}{19}\right)$.

18.2. Calculate $\left(\frac{31}{83}\right)$.

18.3. Let p be odd. Show that $\displaystyle\sum_{k=1}^{p-1/2} k = \frac{p^2-1}{8}$.

18.4. Show that $\frac{p^2-1}{8}$ is an integer, for p an odd number.

18.5. Find the remainder when 17^{51} is divided by 144.

18.6. Show that if $p \geq 5$ is a prime, then $6(p-4)! \equiv 1 \pmod{p}$.

18.7. Show that for any integer a and positive integers m, n, we have

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1.$$

Remark 18.1. We will use

$$\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = \{(x, y) : x \in \mathbb{Z},\ y \in \mathbb{Z}\}$$

to denote the two-dimensional integer integer lattice. The set $\mathbb{Z}^2$ is a subset of the plane $\mathbb{R}^2$. Let p and q be distinct odd primes. As an example, we take $p = 11$ and $q = 7$. Plotted below (see Figure 18.1) are points in the set

$$R = \{(x, y) \in \mathbb{Z}^2 : 0 \leq x \leq p,\ 0 \leq y \leq q\}$$

along with the line ℓ joining $(0, 0)$ with (p, q).

In this plot, the dashed $\frac{p}{2} \times \frac{q}{2}$ rectangle has as vertices the points $(0, 0)$, $(0, \frac{q}{2})$, $(\frac{p}{2}, \frac{q}{2})$, and $(\frac{q}{2}, 0)$. The points inside the rectangle are colored blue.

18.8. Write the equation of the line ℓ.

Remark 18.2. Note that $(p/2, q/2)$ satisfies this equation and hence lies on ℓ.

18.9. Show that, for distinct odd primes p and q, the line ℓ never intersects a point in R (except, of course, $(0, 0)$ and (p, q)).

18.10. For arbitrary p and q, what are the number of points inside the dashed rectangle? In other words, count the number of points in the set

$$R' = \{(x, y) \in \mathbb{Z}^2 : 0 < x < \tfrac{p}{2}, 0 < y < \tfrac{q}{2}\}.$$

Write your answer in terms of p and q.

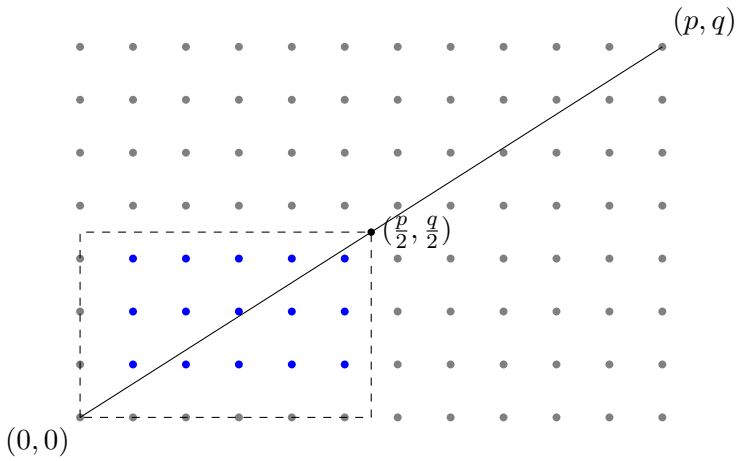


FIGURE 18.1. $p = 11$, $q = 7$

18.11. In Figure 18.1, how many blue points are **above** the line ℓ?

18.12. For $p = 11$ and $q = 7$, compute $\displaystyle\sum_{s=1}^{\frac{q-1}{2}} \left\lfloor \frac{ps}{q} \right\rfloor$.

18.13. In Figure 18.1, how many blue points are **below** the line ℓ?

18.14. For $p = 11$ and $q = 7$, compute $\displaystyle\sum_{s=1}^{\frac{p-1}{2}} \left\lfloor \frac{qs}{p} \right\rfloor$.

18.15. Make a similar figure with $p = 13$ and $p = 11$ How many blue points are **above** the line ℓ?

18.16. For $p = 13$ and $q = 11$, compute $\displaystyle\sum_{s=1}^{\frac{q-1}{2}} \left\lfloor \frac{ps}{q} \right\rfloor$.

18.17. In your figure, how many blue points are **below** the line ℓ?

18.18. For $p = 13$ and $q = 11$, compute $\displaystyle\sum_{s=1}^{\frac{p-1}{2}} \left\lfloor \frac{qs}{p} \right\rfloor$.

Definition 18.3. For odd primes p and q, we denote

$$S(p, q) = \sum_{s=1}^{\frac{q-1}{2}} \left\lfloor \frac{ps}{q} \right\rfloor. \tag{18.1}$$

Remark 18.4. Note that

$$S(q, p) = \sum_{s=1}^{\frac{p-1}{2}} \left\lfloor \frac{qs}{p} \right\rfloor.$$

The last few problems tell us that in Figure 18.1, $S(7,11)$ is the number of points inside the rectangle but above the line ℓ and $S(11,7)$ is the number of points inside the rectangle but below the line ℓ. Since the line ℓ does not intersect with any point inside the rectangle, $S(11,7)+S(7,11)$ is the number of points inside the rectangle R'.

Verify this remark with $S(13,11)$ and $S(11,13)$.

These suggest the following theorem, which you will prove shortly.

Theorem 18.5. *For distinct odd primes p and q, we have*

$$S(p,q)+S(q,p)=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

18.19. For $1\le s\le\frac{q-1}{2}$, argue that the number of points of R' to the right of $(0,s)$ and above the line ℓ is $\left\lfloor\frac{ps}{q}\right\rfloor$.

18.20. Conclude that the number of points in R' above the line ℓ is $S(p,q)$.

18.21. For $1\le s\le\frac{p-1}{2}$, argue that the number of points of R' above $(s,0)$ and below the line ℓ is $\left\lfloor\frac{qs}{p}\right\rfloor$.

18.22. Conclude that the number of points in R' below the line ℓ is $S(q,p)$.

18.23. Prove Theorem 18.5.

Remark 18.6 (Algorithm to find the GCD-II)**.** We can extend the GCD algorithm in Remark 17.1 and obtain x and y such that $nx+my=d$. Once again consider the calculation, but now as a continued fraction:

$$\begin{aligned}\frac{n}{m}&=q_1+\frac{r_1}{m}\\&=q_1+\frac{1}{m/r_1}\\&=q_1+\frac{1}{q_2+r_2/r_1}\\&=q_1+\frac{1}{q_2}+\frac{1}{q_3+r_3/r_2}\\&=\dots\\&=q_1+\frac{1}{q_2}+\frac{1}{q_3}+\dots+\frac{1}{q_n+r_n/r_{n-1}}.\end{aligned}$$

Now we have

$$P_nQ_{n-1}-Q_nP_{n-1}=(-1)^{n+1}a_1\cdots a_n.$$

If we stop in the above calculation when $r_n=d=(m,n)$, then $a_1=a_2=\dots=a_{n-1}=1$ and $a_n=d$. Further, $b_0=q_1$, $b_1=q_2$, ... We find that $P_n=n$, $Q_n=m$, and $x=(-1)^{n-1}Q_{n-1}$, $y=(-1)^nP_{n-1}$. So we can use the recurrence relations for continued fractions to compute x and y.

We define sequences x_n and y_n as follows.

$$x_n=(-1)^{n-1}Q_{n-1},\text{ and }y_n=(-1)^nP_{n-1}.$$

The next few problems will lead you to the **extended GCD algorithm** which simultaneously calculates the GCD d as well as the x and y such that $nx + my = d$.

18.24. Let m and n be given and the notation be as in Remark 18.6. Show that x_n and y_n as above satisfy the following recurrence relations

$$x_k = -q_k x_{k-1} + x_{k-2}, \quad x_{-1} = 1, x_0 = 0, \tag{18.2a}$$

$$y_k = -q_k y_{k-1} + y_{k-2}, \quad y_{-1} = 0, y_0 = 1. \tag{18.2b}$$

Verify that with these initial conditions, $x_1 = 1, y_1 = -q_1$.

Remark 18.7 (Algorithm to find the GCD-II (cont.))**.** Let n and m be given and $n > m$. We can rename $n = r_{-1}$ and $m = r_0$. We have the initial conditions

$$r_{-1} = n, \quad x_{-1} = 1, \ y_{-1} = 0$$

and

$$r_0 = m, \ x_0 = 0, \ y_0 = 1.$$

For $k \geq 1$, we have:

$$q_k = \left\lfloor \frac{r_{k-2}}{r_{k-1}} \right\rfloor \tag{18.3a}$$

$$r_k = -r_{k-1} q_k + r_{k-2}. \tag{18.3b}$$

Calculate for $k = 1, 2, 3, \ldots$ the quantities q_ℓ, r_ℓ, x_ℓ and y_ℓ, until $r_{\ell+1} = 0$. At this point, $d = (n, m) = r_\ell$, and $x = x_\ell$, $y = y_\ell$ are such that $nx + my = d$.

18.25. Find $d = (418, 165)$ and x, y such that $418x + 165y = d$.

PROBLEM SET 19

19.1. Find the highest of power a of 3 that divides 2024!. That is, find a such that $3^a \mid 2024!$ but $3^{a+1} \nmid 2024!$.

19.2. Use the Eratosthenes Sieve to compute all the primes until 40.

19.3. Prove that $\sqrt[3]{7}$ is irrational.

19.4. Find (if possible) the inverse of 6 modulo 19.

19.5. Use a calculator to compute the first few terms of the continued fraction for $\sqrt{3}$.

19.6. Calculate $\varphi(360)$.

19.7. Find$d = (87, 121)$ and x, y such that $87x + 121y = d$.

19.8. Calculate $\displaystyle\sum_{k=0}^{n} \binom{n}{k}$ for $n = 0, 1, 2, 3$. Conjecture and prove a formula.

19.9. Prove that

$$\sum_{k=1}^{n} k^2 = \frac{n\left(n+\frac{1}{2}\right)(n+1)}{3}.$$

19.10. Write 5 as a sum of two squares.

19.11. Write 13 as a sum of two squares.

19.12. Write $65 = a^2 + b^2$ where neither one of a or b is 1.

19.13. Solve $z^4 - 1 = 0$ and plot all the solutions in the complex plane.

We now complete the steps in the proof of Gauss' quadratic reciprocity law. For odd primes p and q such that $p \neq q$, we shall denote

$$p' = \frac{1}{2}(p-1),$$

$$q' = \frac{1}{2}(q-1),$$

and

$$S(q,p) = \sum_{s=1}^{p'} \left\lfloor \frac{sq}{p} \right\rfloor. \tag{19.1}$$

19.14. For integers m and n, show that we can write

$$m = \Big\lfloor \frac{m}{n} \Big\rfloor n + r$$

where $0 \leq r \leq n$.

19.15. Conclude that for $1 \leq k \leq p'$, we can write

$$kq = p\Big\lfloor \frac{kq}{p} \Big\rfloor + u_k$$

where $1 \leq u_k \leq p-1$.

Remark 19.1. Exactly as in the proof of Gauss's lemma, we have that the numbers

$$1q, 2q, \ldots, p'q$$

have least positive residues (modulo p)

$$u_1, u_2, \ldots, u_{p'}.$$

The minimal residues modulo p can be written in the form

$$v_1, \ldots, v_\lambda, -w_1, \ldots, -w_\mu$$

where $\lambda + \mu = p'$, $0 < v_i \leq p'$ and $0 < w_\mu < p'$. The numbers

$$v_1, \ldots, v_\lambda, w_1, \ldots, w_\mu$$

are a rearrangement of the numbers

$$1, 2, \ldots, p'.$$

19.16. Show that

$$\frac{1}{8}(p^2-1) = \sum_{i=1}^{\lambda} v_i + \sum_{j=1}^{\mu} w_j.$$

19.17. Show that

$$\frac{1}{8}(p^2-1)q = pS(q,p) + \sum_{k=1}^{p'} u_k.$$

19.18. Show that

$$\sum_{k=1}^{p'} u_k = \sum_{i=1}^{\lambda} v_i - \sum_{j=1}^{\mu} w_j + \mu p.$$

19.19. Conclude that

$$\frac{1}{8}(p^2-1)(q-1) = pS(q,p) - 2\sum_{j=1}^{\mu} w_j + \mu p.$$

19.20. Using the above equation, show that $S(q,p) \equiv \mu \pmod 2$.

Remark 19.2. You needn't be reminded that $\left(\frac{q}{p}\right)$ is not a fraction but Legendre's symbol.

19.21. Show that

$$\left(\frac{q}{p}\right) = (-1)^{S(q,p)}.$$

19.22. Show that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)}.$$

19.23. Prove Theorem 17.4.

19.24. Given that 200003 is a prime, find the remainder when 200000! is divided by 200003.

19.25. Show that $30 \mid n^5 - n$ for all n.

PROBLEM SET 20

Test

20.1. Find all x such that $4x \equiv 1 \pmod{22}$. If no such x exists, then explain why you think so.

20.2. Find, if possible, a solution of $6x + 22y = 12$. If no such x exists, then explain why you think so.

20.3. Find five consecutive composite numbers.

20.4. Find the number of divisors of 360.

20.5. What is the number of zeros at the end of 2024!.

20.6. Let $n = mq + r$, where $n, m, r > 0$. Show that $(n, m) = (m, r)$.

20.7. Find $\varphi(2024)$ and $\mu(2024)$.

20.8. Show that $2026! \equiv -1 \pmod{2027}$.

20.9. Is 2 a quadratic residue mod 2027?

20.10. Calculate the Legendre symbol

$$\Big(\frac{37}{127}\Big).$$

Explain what it says in terms of quadratic residues.

20.11. Prove, using induction, that for $n \geq 1$

$$x^n - y^n = (x - y)\big(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}\big).$$

20.12. Factor: $x^5 + y^5$ using the above.

20.13. Find the least positive residue of 4^{14} modulo 15.

20.14. Use a calculator to obtain the first ten terms of the simple continued fraction for $e \approx 2.718281828459045\ldots$. What is your guess for the continued fraction of e?

20.15. Find six solutions of the equation $z^6 - 1 = 0$ and plot the solutions in the complex plane.

20.16. How many distinct elements are there in the list

$$1 \cdot 91, 2 \cdot 91, 3 \cdot 91 \cdots, 87 \cdot 91 \pmod{97}.$$

20.17. Show that p divides

$$\binom{p}{\lfloor \frac{p}{2} \rfloor}$$

20.18. Show that the product of a quadratic residue of p and a non-residue of p is a non-residue of p.

20.19. Show that $\left\lfloor \frac{1}{4}(p+1) \right\rfloor$ is odd for a prime of the form $p = 8k \pm 5$.

20.20. Let p be a prime. Calculate

$$\sum_{d|p^{10}} \varphi(d).$$

20.21. Is 5 a prime in $\mathbb{Z}[i]$? If it is is prove it, if not find a prime dividing 5.

20.22. Write 83 as a sum of two squares. If it is not possible to do so, then give a reason.

20.23. Write 89 as a sum of two squares. If it is not possible to do so, then give a reason.

20.24. Let $\gamma = 5 + 4i$ and $\delta = 3 + i$. Find q and r such that $\gamma = \delta q + r$, and $N(r)] \leq \frac{1}{2}N(\delta)$.

20.25. A vendor selling oranges arranges the oranges in stacks of 3 there are two left; when arranging them in stacks of 4, there are three left. When he arranges them in stacks of 7 there is 1 left. What is the minimum number of oranges the vendor has.