SOME INTERESTING ELEMENTARY NUMBER THEORY PROBLEMS

JEREMY BOOHER

1. The Distribution of Primes

(1) Take Euclid's standard proof that there are infinitely many primes (multiply all primes, add one, to get a number with a new prime factor) and use the idea to construct a lower bound on the number of primes less than x. I can get $\log \log x$ up to constant factors. Does the same thing work for primes of the form $4n - 1$?

(2) For any positive integers a and b, define

$$V_{a,b} := \{n \in \mathbb{Z} : n \equiv a \mod b\}.$$

A set $U \subset \mathbb{Z}$ is called open if for every $n \in U$ there is a $V_{a,b}$ such that $n \in V_{a,b} \subset U$. The complement of an open set is called a closed set.

(a) Note that the union of open sets is open. Then show that the intersection of finitely many closed sets is closed. Verify that $\emptyset$ and $\mathbb{Z}$ are closed. This means that the closed sets form a topology on $\mathbb{Z}$.

(b) Show that $T = \{n \in \mathbb{Z} : n \text{ does not has a prime divisor}\} = \{\pm 1\}$ is not an open set. (Note that closed $\neq$ not open)

(c) Show that all open sets are closed. Deduce from this and the fact that T is not closed that there are infinitely many primes

(3) Suppose there are only finitely many primes $p_1, p_2, \ldots, p_m$. Let S_N be the set of all positive integers of the form $\prod p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}$ that are less than 2^N. Estimate the maximum size of the e_i. How many elements are there in S_N? Deduce yet again that there are an infinite number of primes.

(4) The prime number theorem says the number of primes less than or equal to x, denoted by $\pi(x)$, is asymptotically equal to $\frac{x}{\log(x)}$. It is not easy to prove. But here is a much easier argument to due Chebyshev that says

$$\log 2 \cdot \frac{x}{\log(x)} + O(1) < \pi(x) < 2 \log 2 \cdot \frac{x}{\log(x)} + O(\log(x)).$$

Chebyshev's idea is to use the van Mangoldt function $\Lambda(n)$, (defined to be $\log(p)$ if $n = p^r$ and p is prime, 0 otherwise) to define $\psi(x) := \sum_{n \leq x} \Lambda(n)$. $\psi(x)$ is easier to analyze.

(a) Show that

$$\psi(x) \leq \pi(x) \log(x).$$

Therefore a lower bound on $\psi(x)$ gives a lower bound on $\pi(x)$.

(b) Furthermore, show that for any $\epsilon > 0$,

$$\psi(x) \geq \sum_{x^{1-\epsilon} \leq p \leq x} \log(p) \geq (1 - \epsilon)(\pi(x) - x^{1-\epsilon}) \log(x)$$

and so

$$\pi(x) \log(x) \leq \frac{1}{1 - \epsilon} \psi(x) + \log(x) x^{1-\epsilon}.$$

Date: Mostly Summer 2010.

Let ϵ go to 0 to conclude

$$\pi(x) \leq \frac{\psi(x)}{\log(x)} + O(1).$$

(c) Establish Chebyshev's key observation, that

$$\log(x!) = \sum_{n=1}^{\infty} \left[\frac{x}{n}\right] \Lambda(n).$$

(d) Show that the following string of inequalities holds:

$$\psi(2n) \geq \sum_{k=1}^{\infty} (-1)^{k+1} \psi(2n/k) = \log\left(\frac{(2n)!}{(n!)^2}\right) = \log(2)(2n) + O(\log(n)).$$

You may find Stirling's formula useful: there is a constant C for which

$$\log(x!) = (x + \frac{1}{2})\log(x) - x + C + O(\frac{1}{x}).$$

(e) Now show that

$$\psi(x) \leq \log(x!) - \sum_{n=1}^{\infty} \log\left(\left[\frac{x}{2^n}\right]!\right).$$

Conclude that

$$\psi(x) \leq \sum_{m=1}^{\infty} \frac{m}{2^m} \log(2)x + O(\log^2(x)) = 2\log(2)x + O(\log^2(x)).$$

(f) Establish the bounds on $\pi(x)$.

(5) PODASIP: $\sum_{p \text{ prime}} \frac{1}{p}$ is a divergent series.

You may find the following facts useful intermediate steps:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} \quad \text{for } s > 1$$

$$|-\log(1-x) - x| \leq Cx^2 \quad \text{for a constant } C \text{ and small } x.$$

(6) Dirichlet's theorem specializes to a reasonably simple argument when looking at primes of the form $4n+1$ and $4n-1$. Be careful not to rearrange series unless they are absolutely convergent.

(a) Show that $1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \ldots = \frac{\pi}{4}$ by integrating the power series for $\frac{1}{1+x^2}$ term by term and evaluating the integral directly.

(b) Let $\chi_4(n) = 1$ if $n \equiv 1 \mod 4$, -1 if $n \equiv -1 \mod 4$, and 0 otherwise. Show that for $s > 1$

$$\sum_{n=1}^{\infty} \frac{\chi_4(n)}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - \chi_4(p)p^{-s}}.$$

(c) Show that $\lim_{s \to 1^+} \sum_{p \text{ prime}} -\log(1 - \chi_4(p)p^{-s})$ exists.

(d) Show that $\sum_{p \text{ prime}} \frac{\chi_4(p)}{p^s} = \sum_{p \text{ prime}} \frac{1}{p^s} - 2 \sum_{p \equiv 3 \mod 4} \frac{1}{p^s}$ exists as $s \to 1^+$.

(e) There are infinitely many primes of the form $4n + 3$. Can you do the same for $4n + 1$?

(7) The standard way to prove there are infinitely many primes of the form $4n+1$ is to assume their are a finite number, and let their product P. By looking at x^2+1 evaluated at $2P$ conclude there is another prime of the same form.

Suppose Q be the product of the finite number of primes of the form $5n+1$. Try looking at $x^4+x^3+x^2+x+1$ evaluated at $5Q$ to show there are infinitely many primes of the form $5n+1$. For which other m does this show there are infinitely many primes congruent to 1 modulo m?

2. Generators

(8) Let p be a prime, and form a $p-1$ by $p-1$ grid where the ith column is the powers of i modulo p. If a row is not all 1s, pick an element a for which $a^k \neq 1$. Multiplying by a permutes the columns. What is the sum of a row? What is the sum of each column?

Use this information to find elements of order q for every prime power q dividing $p-1$. Show that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. Does this generalize to prime power moduli?

	1	2	3	4
a^0	1	1	1	1
a^1	1	2	3	4
a^2	1	4	4	1
a^3	1	3	2	4

Table 1. The grid when $p=5$

(9) Show that the element $1+p$ has order p^{k-1} in $(\mathbb{Z}/p^k\mathbb{Z})^\times$ by looking at the Frobenius map $(\mathbb{Z}/p^k\mathbb{Z})^\times \to (\mathbb{Z}/p^k\mathbb{Z})^\times$ that sends $a \to a^p$.
Find an element of order $p-1$ in $(\mathbb{Z}/p^k\mathbb{Z})^\times$. Conclude that $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic.

(10) For which positive integers n is $(\mathbb{Z}/n\mathbb{Z})^\times$ cyclic?

(11) PODASIP: $(\mathbb{Z}[i]/(\pi))^\times$ is cyclic iff $(\mathbb{Z}/(N(\pi)))^\times$ is cyclic. There is also an isomorphism between $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}/(N(\pi))$.

3. Computing Square Roots Modulo n

(12) The purpose of this problem is to show how to compute the square root of an integer modulo p efficiently. Let p be a prime and a be a quadratic residue modulo p.

(a) Suppose $p \equiv 3 \mod 4$. Since $\frac{p+1}{4}$ is an integer, show how to trivially compute a square root of a modulo p.

(b) Let $p-1 = 2^r s$ with $s \equiv 1 \mod 2$. Let v be a quadratic non-residue modulo p. Set $w = v^s$ and $x_0 = a^{\frac{s+1}{2}} \mod p$. Show that $\operatorname{ord}(x_0^2/a) = 2^{t_0}$, where $0 \le t_0 \le r$. (Here $\operatorname{ord}(x)$ denotes the order of x modulo p, the smallest positive integer for which $x^n = 1 \mod p$.)

(c) Recursively define $x_{i+1} = x_i w^{2^{r-t_i-1}}$. Show that $\operatorname{ord}(x_{i+1}^2/a) = 2^{t_{i+1}}$ for t_{i+1} a non-negative integer.

(d) Show that x_i will eventually be a square root of a. What is an upper bound on the number of iterations this will take? To be efficient, this algorithm needs to run in time bounded by a polynomial in the size on the input. The size of the input is the number of digits in p, so this algorithm needs to do at most $f(\log(p))$ steps, where f is a polynomial. Show this algorithm is efficient, as long as we are given a quadratic non-residue modulo p.

(e) Show how to find a quadratic non-residue modulo p easily using randomness. (There is no known algorithm that is provably efficient and does not use randomness.)

(f) Now that we know how to compute square roots modulo p, show how to compute square roots modulo a composite modulus n provided we already know the prime factorization of n.

(13) However, computing square roots is hard to do without knowing the factorization of n. The following encryption method, called Rabin encryption, exploits this.

Let n be a product pq of primes congruent to $3 \mod 4$. n is publicly available. Alice sends Bob a message by looking up his public key n. She encodes the message as one (or more) integers modulo n. She squares M to get the cipher text $C = M^2 \mod n$. She sends Bob C.

(a) Show how Bob, who knows p and q, can recover M easily.

(b) Suppose Eve can somehow decrypt messages that Alice sends Bob efficiently. Show how Eve can use her decryption method to factor n. Most of modern public key cryptography is based on the intractability of factoring large numbers, so this is a reasonable level of security. No one knows how to factor n easily, but no one can prove it is hard either.

(14) As an alternative to using randomness to find a quadratic non-residue modulo p, one could simply check $1, 2, 3 \ldots \mod p$ until you find a non-residue. An interesting question is what we can say about the smallest non-residue modulo p.

To make this a meaningful question, say that the smallest quadratic non-residue is $O(f(p))$ if there is a constant C such that the smallest quadratic non-residue is less than $C \cdot f(p)$ for all but finitely many primes p.

Show that the smallest quadratic non-residue is $O(p^{\frac{1}{2}})$ by using the fact that the product of quadratic residues is a quadratic residue and that half of the integers modulo p are quadratic residues.

4. Arithmetic Functions and Character Sums

(15) An alternate approach to bounding the smallest quadratic non-residue is to consider the character character sum

$$S_\chi(N) := \sum_{n=1}^{N} \chi(n).$$

The Pólya-Vinogradov bound says that $|S_\chi(N)| \leq Cp^{\frac{1}{2}} \log(p)$ for some constant C. Here we take $\chi(n) = \left(\frac{n}{p}\right)$.

(a) Use the Pólya-Vinogradov bound to prove that the smallest quadratic non-residue is $O(p^{\frac{1}{2}} \log(p))$.

(b) Let χ be any non-trivial character on $(\mathbb{Z}/p\mathbb{Z})^\times$: in other words, let $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ such that $\chi(ab) = \chi(a)\chi(b)$ and χ is not uniformly 1. Prove that

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \overline{\chi}(a) e^{2\pi i n a/p}$$

where the Gauss sum $\tau(\overline{\chi})$ is defined as

$$\tau(\overline{\chi}) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \overline{\chi}(a) e^{2\pi i a/p}.$$

(This is a statement about finite Fourier series.)

(c) Using this, show that

$$S_\chi(N) = \frac{-1}{\tau(\overline{\chi})} \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \overline{\chi}(a) \frac{1 - e^{2\pi i N a/p}}{1 - e^{-2\pi i a/p}}.$$

(d) Show that for any non-trivial character χ,

$$|\tau(\chi))|^2 = \tau(\chi)\overline{\tau(\chi)} = p$$

(e) Conclude that $|S_\chi(N)| \leq Cp^{\frac{1}{2}} \log(p)$.

Remark 1. The state of the art unconditional bound is $O(p^{\frac{1}{4\sqrt{e}}+\epsilon})$. Vinagradov conjectured it is actually $O(p^\epsilon)$.

(16) Quadratic reciprocity is also connected with Gauss sums, defined as

$$\tau(\chi) = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi(a)e^{2\pi ia/p}.$$

We are interested in the case when $\chi = \chi_q := \left(\frac{\cdot}{q}\right)$.

A way to establish the supplemental law $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}}$ without Gauss's lemma is to look at $(1+i)^{p-1}$ in $\mathbb{Z}[i]_p$. Use Euler's criteria and the observation that $(1+i)^{p-1} = (2i)^{\frac{p-1}{2}}$, so $(1+i)$ is almost a square root of 2.

Prove quadratic reciprocity for odd primes by using the fact that $\tau(\chi_q)$ is almost a square root of q (see 15d). Be wary of problem 33.

(17) Given a multiplicative function $f(n)$, let $P_f(T)$ denote the formal Dirichlet series

$$P_f(s) := \sum_{n=1}^{\infty} f(n)n^{-s}.$$

What is $P_f(s) \cdot P_g(s)$? Is it P_h for some arithmetic function h?

Show that $P_f(s)$ has an inverse in the ring of Dirichlet series. What does this say about $f(n)$? What kind of algebraic structure can you put on multiplicative functions?

(18) Define the Mangoldt function as $\Lambda(n) = \log p$ if $n = p^m$ (p a prime and $m \geq 1$), 0 otherwise.

Show that $\log(n) = \sum_{d|n} \Lambda(d)$ and that $\Lambda(n) = \sum_{d|n} \mu(d)\log(\frac{n}{d})$.

Establish the Selberg identity, which is a starting point for an "elementary" proof of the prime number theorem.

$$\Lambda(n)\log(n) + \sum_{d|n} \Lambda(d)\Lambda(\frac{n}{d}) = \sum_{d|n} \mu(d)\log^2(\frac{n}{d})$$

Hint: For an arithmetic function $f(n)$, consider differentiating the associated Dirichlet series.

(19) Let p be an odd prime. Count the number of solutions to $x^2 + y^2 = m \mod p$ by evaluating

$$\sum_{a+b=m} \left(1 + \left(\frac{a}{p}\right)\right)\left(1 + \left(\frac{b}{p}\right)\right)$$

where the sum is over $a, b \in (\mathbb{Z}/p\mathbb{Z})$. Do the same for $x^2 + y^2 + z^2 + w^2 = m \mod p$.

(20) In contrast to ternary quadratic forms (see problem 27), the equation $3x^3 + 4y^3 + 5z^3 = 0$ has no non-trivial rational solutions but it does have non-trivial solutions modulo p and over $\mathbb{R}$. One can prove the second assertion using character sums.

Notation: $\mathbb{F}_p$ will denote the finite field with p elements, also denoted $\mathbb{Z}/p\mathbb{Z}$. χ will be a group homomorphism $\mathbb{F}_p^\times \to \mathbb{C}^\times$: an example is the Legendre symbol. ψ will be a group homomorphism $\mathbb{F}_p \to \mathbb{C}^\times$: an example is $a \to e^{2\pi a/p}$.

Note that solutions (a, b, c) to $3a^3+4b^3+5c^3 = 0 \mod p$ come in groups of $p-1$: $(\lambda a, \lambda b, \lambda c)$ is also a solution for $\lambda \neq 0$. $(0, 0, 0)$ is also a solution. Thus the total number of solutions is $1 + (p-1)N$ for some N.

(a) Show that

$$\sum_{a,b,c\in\mathbb{F}_p}\sum_{\psi:\mathbb{F}_p\to\mathbb{C}^\times}\psi(3a^3+4b^3+5c^3)=p(1+(p-1)N).$$

(b) Show that

$$p(1+(p-1)N)=p^3+\sum_{\psi\neq 1}\left(\sum_{a\in\mathbb{F}_p}\psi(3a^3)\right)\left(\sum_{b\in\mathbb{F}_p}\psi(4b^3)\right)\left(\sum_{c\in\mathbb{F}_p}\psi(5c^3)\right).$$

(c) If $p\neq 1 \mod 3$, show that $N=p+1$.

(d) Otherwise, assume $p\equiv 1 \mod 3$. Show that

$$\sum_{a\in\mathbb{F}_p}\psi(\lambda a^3)=1+\sum_{a\in\mathbb{F}_p^\times}\psi(a)+\sum_{\chi\neq 1,\chi^3=1}\chi(\lambda)^{-1}\sum_{a\in\mathbb{F}_p}\chi(a)\psi(a).$$

The last sum

$$\tau(\chi,\psi)=\sum_{a\in\mathbb{F}_p}\chi(a)\psi(a)$$

is a slight generalization of a Gauss sum. Note there are only three solutions to $\chi^3=1$ for $\chi\in\hat{\mathbb{F}_p}$.

(e) Conclude that $p(1+(p-1)N)-p^3=$

$$\left(\sum_{\psi\neq 1}\overline{\chi(3)}\tau(\chi,\psi)+\chi(-3)\overline{\tau(\chi,\psi)}\right)\left(\sum_{\psi\neq 1}\overline{\chi(4)}\tau(\chi,\psi)+\chi(-4)\overline{\tau(\chi,\psi)}\right)\left(\sum_{\psi\neq 1}\overline{\chi(5)}\tau(\chi,\psi)+\chi(-5)\overline{\tau(\chi,\psi)}\right)$$

which simplifies to

$$\sum_{\psi\neq 1}\overline{\chi}(60)\tau(\chi,\psi)^3+\chi(-60)\overline{\tau(\chi,\psi)}^3.$$

Solve for N.

(f) Show that $|N-(p+1)|\leq 2\sqrt{p}$ and conclude that $N>0$. Thus $3x^3+4y^3+5z^3=0 \mod p$ has a non-trivial solution.

5. Minkowski's Theorem

(21) Minkowski's theorem says that if Ω is a convex, symmetric body with area bigger than 4, then it contains a lattice point besides the origin. What happens if the area is exactly 4?

(22) Let Λ be a lattice in $\mathbb{R}^n$ generated by the vectors $\vec{v}_1,\vec{v}_2,\ldots,\vec{v}_n$. Show that the area of the fundamental domain for the lattice is

$$\det\begin{pmatrix}\vec{v}_1 & \vec{v}_2 & \ldots & \vec{v}_n\end{pmatrix}.$$

(23) Prove the 2 and 4 squares theorem using Minkowski's theorem. Hint: use elements that satisfy $a^2=-1 \mod p$, $b^2+c^2+1=0 \mod p$ to construct a lattice.

(24) Show how to prove that if $p\equiv 1 \mod 4$ then p is a sum of two squares in a unique way (up to signs and ordering) follows from the lattice used in the proof of the existence result via Minkowski's theorem. Hint: Pick's theorem

(25) Given $\alpha_1,\ldots,\alpha_r$ in $\mathbb{R}$ and $n>0$, let C denote the subset of $\mathbb{R}^{r+1}$ such that

$$|x_0|<n+1 \quad\text{and}\quad |\alpha_i x_0-x_i|<n^{-\frac{1}{r}}.$$

Conclude there exist $a_1,\ldots,a_r,b\in\mathbb{Z}$ with $0<b\leq n$ such that

$$\left|\frac{a_i}{b}-\alpha_i\right|<\frac{1}{bn^{\frac{1}{r}}}.$$

What does this say when $r = 1$?

6. Local to Global Principals

A major idea in algebraic number theory is to find a way to use local information such as solutions of an equation modulo p to deduce information about integral solutions.

(26) Show that the only integral solutions to $x^2 - 5y^2 - 3z^2 = 0$ is $(x, y, z) = 0$.

(27) The Hasse Principle for quadratic forms states that a quadratic form in three variables represents 0 non-trivially if and only if it non-trivially represents 0 modulo p for every odd prime and modulo 8.

(a) Let $Q(x_1, x_2, x_3)$ be a ternary quadratic form with rational coefficients. Show that we may assume it is of the form $a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ where $a_1, a_2, a_3 \in \mathbb{Z}$ and $a_1a_2a_3$ is nonzero and square free.

(b) If $p \neq 2$ and $p|a_3$, show there exists $r \in \mathbb{Z}$ such that $r^2a_1 + a_2 \equiv 0 \mod p$.

(c) If $p = 2$ and $2 \not| a_1a_2a_3$, show that after re-indexing the a_i we have $a_1 + a_2 \equiv 0 \mod 4$. If $2|a_3$, then there exists an $s = 0, 1$ such that $a_1 + a_2 + s^2a_3 \equiv 0 \mod 8$.

(d) Impose congruence conditions to obtain a lattice. Use Minkowski's theorem to find a triple $(x_1, x_2, x_3) \neq (0, 0, 0)$ such that $Q(x_1, x_2, x_3) = 0$.

(e) Note that the above proof does not need to use all primes, only a finite number. So let p and q be distinct odd primes. Suppose $q \equiv 3 \mod 4$ and that $\left(\frac{-p}{q}\right) = 1$. This says that

$$x_1^2 + px_2^2 + qx_3^2 = 0$$

has a nontrivial solution modulo q. But the equation clearly has no rational solutions. Conclude there can be no solutions modulo p. How much of quadratic reciprocity can you deduce from this idea?

There is a similar statement for quadratic forms in four or more variables, but the only proof I know requires Dirichlet's theorem on primes in arithmetic progressions and knowledge about local fields. It can be used to deduce the three square theorem.

(28) Show that the equation $(x^2 - 2)(x^2 + 1)(x^2 + 2) = 0 \mod n$ has solutions for every positive integer n but that it has no integral solutions.

(29) Can you do the same for an irreducible polynomial in $\mathbb{Z}[x]$?

(30) Consider the equation $x^2 - 142y^2 = 19$.

(a) Consider the equation $x^2 - 142y^2 = 19 \cdot 9$. Find an integer solution. Deduce there are rational solutions to $x^2 - 142y^2 = 19$.

(b) Show there are solutions modulo m for any m with $(m, 3) = 1$.

(c) Show there are solutions modulo 3^r for any $r \geq 1$. Conclude there are solutions modulo n for any n.

(d) Show there are no integral solutions.
Suggested Strategy: Find a solution (x_1, y_1) to $x_1^2 - 142y_1^2 = 1$ in integers. Suppose (x_0, y_0) is a solution to $x^2 - 142y^2 = 19$. Working in $\mathbb{Q}(\sqrt{142})$, show

$$(x_0x_1 - 142y_0y_1, x_1y_0 - x_0y_1)$$

is also a solution to $x^2 - 142y^2 = 19$.

(31) PODASIP: $p = x^2 + ny^2$ if and only if $\left(\frac{-n}{p}\right) = 1$. What can you say about other quadratic forms like $2x^2 + 2xy + 3y^2$?

7. Rings of Integers

(32) Let $n \equiv 1 \mod 4$. Compute the number of ways to write n in the form $x^2 + 4y^2$ with $x, y > 0$ for all $n \leq 30$. Any conjectures? Can you prove them by looking in $\mathbb{Z}[i]$?

Try the same thing for $3x^2 + y^2$.

(33) Consider all expressions of the form $a_0+a_1\zeta_5+a_2\zeta_5^2+a_3\zeta_5^3+a_4\zeta_5^4$, where ζ_5 is a fifth root of unity. This is an analogy of $\mathbb{Z}[i]$ for a different root of unity. PODASIP: If $a_0+a_1\zeta_5+a_2\zeta_5^2+a_3\zeta_5^3+a_4\zeta_5^4$ is a multiple of p if and only if all of the a_i are multiples of p.

(34) Let $K=\mathbb{Q}(\sqrt{d})$, with d square free. Let $\mathcal{O}_K$ denote all elements of K that are solutions to monic polynomials with integral coefficients. Find an explicit description of $\mathcal{O}_K$.

(35) Describe the primes in $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ using similar ideas to the way we described primes of $\mathbb{Z}[i]$.

(36) For which $K=\mathbb{Q}(\sqrt{d})$ can you show $\mathcal{O}_K$ is a Euclidean domain?

(37) Let $\alpha\in\mathcal{O}_K$. Show that $|\mathcal{O}_K/\alpha|=N(\alpha)$.

(38) Find all integral solutions to $y^2+4=z^3$. Hint: $\mathbb{Z}[i]$

(39) $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ has unique prime factorization, but it is not a Euclidean domain. The standard proof that it has unique prime factorization would require significant algebraic number theory or theory about quadratic forms. This problem will prove it is not Euclidean using the idea of universal side divisors, and show it has UPF by showing it admits a Dedekind-Hasse norm.

   (a) For a ring R, let $\tilde{R}$ denote the units of R and 0. A universal side divisor is an element $u\in R-\tilde{R}$ such that for any $x\in R$ there exists a $q\in R$ and $z\in\tilde{R}$ such that $x=uq+z$. Show that if R is an integral domain that is not a field, then R being Euclidean implies there are universal side divisors in R.

   (b) Show that $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ has no universal side divisors. Suggested strategy: the norm of $a+b\left(\frac{1+\sqrt{-19}}{2}\right)$ is $a^2+ab+5b^2$. Find the elements of small norm. Try taking $x=2$ in the definition of universal side divisor, and restricting the possible choices of a universal side divisor u. Try taking $x=\frac{1+\sqrt{-19}}{2}$ and deduce there are no universal side divisors.

   (c) A Dedekind-Hasse norm is a function $N:R\to\mathbb{N}\cup\{0\}$, with $N(\alpha)=0$ only if $\alpha=0$, and such that for every non-zero $a,b\in R$ then a is a multiple of b or there exist $s,t\in R$ with $0<N(sa-tb)<N(b)$. Show that a Euclidean domain has a Dedekind-Hasse norm. Show that every ideal of R is principal if R admits a Dedekind-Hasse norm.

   (d) Show that the norm $N\left(a+b\left(\frac{1+\sqrt{-19}}{2}\right)\right)=a^2+ab+5b^2$ is a Dedekind-Hasse norm.

(40) Minkowski's theorem can be used to prove Dirichlet's Unit theorem for real quadratic fields. It states that for $K=\mathbb{Q}(\sqrt{d})$ with $d>0$ and square-free, the unit group of $\mathcal{O}_K$ is isomorphic to $\{\pm 1\}\times\mathbb{Z}$. The generator of the infinite cyclic part is called a fundamental unit.

Embed $\mathbb{Q}(\sqrt{d})$ in $\mathbb{R}^2$ by sending $a+b\sqrt{d}\in\mathbb{Q}(\sqrt{d})$ to $(a+b\sqrt{d},a-b\sqrt{d})\in\mathbb{R}^2$. Show that under this map $\mathcal{O}_K$ embeds as a lattice in $\mathbb{R}^2$. The norm of $a+b\sqrt{d}$ is now xy. Identify the units in this picture. Use Minkowski's theorem and the pigeonhole principal to find a non-trivial unit. Then argue that $\mathcal{O}_K\simeq\{\pm 1\}\times\mathbb{Z}$.

However, this argument doesn't generalize to other number fields. Instead, use Minkowski's theorem to show there are two units u_1 and u_2 with the x-coordinate of u_1 less than 1 and the y-coordinate of u_2 less than 1.

Embed $\mathbb{Q}(\sqrt{d})$ in $\mathbb{R}^2$ by sending $a+b\sqrt{d}$ to $(\log|a+b\sqrt{d}|,\log|a-b\sqrt{d}|)$. Show that $\log(|N(a+b\sqrt{d})|)=x+y$ under this embedding, and all units lie on a line. Let u_1 embed as (x_1,y_1) and u_2 embed as (x_2,y_2). Show that the matrix

$$\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$$

has rank 1 using the fact that $x_i+y_i=0$ and $x_1<0$ and $y_2<0$. Deduce Dirichlet's unit theorem for $\mathbb{Q}(\sqrt{d})$.

Try to generalize this argument to $\mathbb{Q}(\sqrt{r},\sqrt{s})$ where $r,s>0$. Dirichlet's theorem predicts a rank 3 unit group.

8. Reciprocity Laws

(41) We can reinterpret the proof of quadratic reciprocity in (16) in terms of finite fields.

(a) Let $\mathbb{F}_q$ denote the field with p^r elements, where p is a prime. Show that $\mathrm{Frob}_p : \mathbb{F}_q \to \mathbb{F}_q$ defined by $x \to x^p$ is a bijective ring homomorphism. It is called the Frobenius.

(b) Show that for $x \in \mathbb{F}_q$, $\mathrm{Frob}_p(x) = x$ if and only if $x \in \mathbb{F}_p \subset \mathbb{F}_q$.

(c) Let p and p' be odd primes. Show there is a finite field $\mathbb{F}_q = \mathbb{F}_{p^n}$ for which $x^{q'} - 1$ has q' solutions in $\mathbb{F}_p$. (This is called the splitting field of $x^{q'} - 1$.) Denote these solutions by $1, \zeta_{p'}, \zeta_{p'}^2, \ldots, \zeta_{p'}^{p'-1}$. Note these are not complex numbers, despite being roots of unity.

(d) Let $\chi_{p'}(a) = \left(\frac{a}{p'}\right)$. Define the Gauss sum

$$g(\chi_{p'}) = \sum_{a \mod p'} \chi_{p'}(a)\zeta_{p'}^a.$$

Mimicking the proof of (15d), show that $g(\chi_{p'})^2 = p'$ in $\mathbb{F}_q$.

(e) Show that p' has a square root modulo p if and only if $\mathrm{Frob}_p(g(\chi_{p'})) = g(\chi_{p'})$.

(f) Mimick the proof in (16) to simplify $\mathrm{Frob}_p(g(\chi_{p'}))$ and deduce quadratic reciprocity.

(42) Can formulate an analogue of quadratic reciprocity for third powers? It may be easiest to work in $\mathbb{Z}[\zeta_3]$, where $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$, since all of the third roots of unity exist ((35) may be helpful). A helpful convention: just as we work with positive primes as opposed to negative ones in $\mathbb{Z}$, we need a prefered choice of associates in $\mathbb{Z}[\zeta_3]$. The standard convention is to work with primary primes, which are primes $\pi \in \mathbb{Z}[\zeta_3]$ for which $\pi \equiv 2 \mod 3$. Check that exactly one associate of every prime is primary (except those dividing 3).

You can prove it using a similar technique to the Gauss sum approach to quadratic reciprocity. For a prime π and $\alpha \in \mathbb{Z}[\zeta_3]$. Let ζ_3^m be the unique root of unity such that $\alpha^{(N\pi-1)/3} \equiv \zeta_3^m \mod \pi$. Define the cubic residue character to be

$$\left(\frac{\alpha}{\pi}\right)_3 := \zeta_3^m.$$

If $\pi|3$, define $\left(\frac{\alpha}{\pi}\right)_3 := 0$.

Let π be a primary prime of $\mathbb{Z}[\zeta_3]$ that is not rational, and let p be a prime of $\mathbb{Z}[\zeta_3]$ that is also prime in $\mathbb{Z}$. Define $p' = N(\pi)$. Denote the conjugate of π by $\overline{\pi}$, so $\pi\overline{\pi} = p'$.

(a) Using (37), show that elements of $\mathbb{Z}[\zeta_3]$ naturally give elements of $\mathbb{Z}[\zeta_3]/(p) \simeq \mathbb{F}_{p^2}$. In particular, π is a cube modulo p iff and only if its reduction is a cube in $\mathbb{F}_{p^2}$.

(b) Let $\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3$ denote the cubic residue character. How does it become a character of $\mathbb{F}_{p'}$? It takes on the values $1, \zeta_3, \zeta_3^2$: interpret them as elements of $\mathbb{F}_{p^2}$.

(c) Pick an extension $\mathbb{F}_{p^2} \subset \mathbb{F}_{p^n}$ that contains the p'th roots of unity. Define the Gauss sum

$$g(\chi_\pi) = \sum_{a \in \mathbb{F}_{p'}} \left(\frac{a}{\pi}\right)_3 \zeta_{p'}^a.$$

Verify that $g(\chi_\pi)^2 = p'$ in $\mathbb{F}_{p^n}$.

(d) Define the Jacobi sum

$$J(\chi_\pi, \chi_\pi) = \sum_{x+y=1 \mod p'} \chi_\pi(x)\chi_\pi(y).$$

This can be interpreted either as a complex number in $\mathbb{Z}[\zeta_3]$ or an element of a finite field. The first reduces modulo p to the second. Show that $g(\chi_\pi)^3 = p'J(\chi_\pi, \chi_\pi)$ and $J(\chi_\pi, \chi_\pi)$ is a primary prime in $\mathbb{Z}[\zeta_3]$.

(e) Show that $J(\chi_\pi, \chi_\pi) = \pi$ and consequently $g(\chi_\pi)^3 = \pi^2\overline{\pi} = p'\pi$ (in $\mathbb{F}_{p^2} \simeq \mathbb{Z}[\zeta_3]/(p)$).

(f) Show that p' is always a cube in $\mathbb{F}_{p^2}$. Thus π is a cube if and only $g(\chi_\pi) \in \mathbb{F}_{p^2}$.

(g) Define $\text{Frob}_{p^2} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ by raising to the p^2-power. Show $g(\chi_\pi) \in \mathbb{F}_{p^2}$ if and only if $\text{Frob}_{p^2} g(\chi_\pi) = g(\chi_\pi)$.

(h) Simplify $\text{Frob}_{p^2} g(\chi_\pi)$ and deduce a case of cubic reciprocity.

(i) Deal with the case of two rational primes (elements of $\mathbb{Z}$), and the case of two primary primes that are not rational by similar arguments to prove the full cubic reciprocity law.

Can you formulate and prove supplemental laws for $1 - \zeta_3$ and the units of $\mathbb{Z}[\zeta_3]$?

(43) Is there a law of biquadratic (fourth power) reciprocity?

(44) Consider $(\mathbb{Z}/7\mathbb{Z})^\times$. There are six elements - $1, 2, 3, 4, 5, 6$ - and multiplication by 2 permutes them.

$$1 \to 2 \quad 2 \to 4 \quad 3 \to 6 \quad 4 \to 1 \quad 5 \to 3 \quad 6 \to 5$$

We can write this down in cycle notation as (124)(365). The sign of the permutation is defined two equivalent ways: either as $(-1)^{n_1-1+n_2-1+\ldots+n_o-1}$ where the permutation is made up of cycles of length $n_1, n_2, \ldots, n_o$ or as the parity of the number of inversions. The numbers $1, 2, 3, 4, 5, 6$ are ordered. The permutation σ has an inversion when $i < j$ and $\sigma(i) > \sigma(j)$. For example, since multiplication by 2 is a product of two three cycles, it has sign $(-1)^{3-1+3-1} = 1$. Likewise, the following pairs are all the inversions: $(1, 4)$, $(2, 4)$, $(2, 5)$, $(3, 4)$, $(3, 5)$, $(3, 6)$, so the sign is again seen to be 1.

(1) Calculate the sign of the permutations obtained by multiplying by $1, 2, 3, 4, 5, 6$ modulo 7. Do the same thing modulo 11 and 13. What patterns do you see? Prove them. Does it matter if we include 0?

(2) What is the sign of the permutation that sends $a \to a + b \mod n$?

Let $S_{m,n} = \{0, 1, 2, \ldots, m - 1\} \times \{0, 1, 2, \ldots, n - 1\}$. Given a pair $(a, b) \in S_{m,n}$, find x and y such that $x \equiv an + b \mod m$ and $ym + x \equiv b \mod n$ where $0 \leq x < m$ and $0 \leq y < n$. Map (a, b) to (x, y). Interpret this as mapping the kth element of $S_{m,n}$ to the kth element of $S_{m,n}$ under two different orderings: order lexigraphically based on the first or second coordinate. If $m = 2$ and $n = 3$, then

$$(0, 0) \to (0, 0) \quad (0, 1) \to (1, 0) \quad (0, 2) \to (0, 1) \quad (1, 0) \to (1, 1) \quad (1, 1) \to (0, 2) \quad (1, 2) \to (1, 2)$$

which has sign -1. Call this permutation λ.

(3) Calculate the sign of this permutation for $(m, n) = (2, 5)$, $(3, 4)$, and $(5, 6)$. How can you predict the sign of λ in terms of m and n?

Let p and q be odd primes with $p < q$, and consider the following permutation of $S_{p,q}$:

- λ, as defined above.
- α, which sends $(x, y) \to (qx + y, y)$.
- β, which sends $(x, y) \to (x, x + py)$.

(4) Write down these permutation and find their signs for $(p, q) = (3, 5)$, $(3, 7)$, and $(5, 11)$. How is this illustrating quadratic reciprocity? Use this idea to prove the theorem in general.

(45) Let p and q be odd primes. Consider $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})^\times$, with subgroup $A = \{(\pm 1, \pm 1)\}$. Let $S = \{(a, b) : 1 \leq a < p, 1 \leq b \leq \frac{q-1}{2}\}$. (These are coset representatives.) Let P be their product:

$$P = \prod_{(a,b) \in S} (a, b). = \left((p - 1)!^{\frac{q-1}{2}}, \left(\frac{q - 1}{2} \right)!^{p-1} \right) \in (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})^\times$$

Let T be an alternate set of coset representatives, $T = \{(k \mod p, k \mod q) : 1 \leq k \leq \frac{pq-1}{2} (k, pq) = 1\}$, and let

$$P' = \prod_{(a,b) \in T} (a, b).$$

(a) Show that $P = ((p - 1)!^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}\frac{q-1}{2}} (q - 1)!^{\frac{p-1}{2}}) \in (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})^\times$.

(b) Show that $P = \pm P'$ in $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})^\times$.

(c) Calculate P' by directly taking the product in each component, so

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

(d) Deduce quadratic reciprocity.

9. Continued Fractions

All of these questions relating to continued fractions may be false. Prove or disprove and salvage if possible. The interesting case is usually when β is irrational.

(46) If $\frac{p_n}{q_n}$ is the nth convergent to β and

$$\left|\beta - \frac{p}{q}\right| < \frac{1}{2q_n^2}$$

then $q \geq q_{n+1}$.

(47) There are infinitely many rational solutions $\frac{p}{q}$ to

$$\left|\frac{p}{q} - \beta\right| < \frac{1}{\sqrt{5}q^2}.$$

(48) Let $\beta = \frac{-1+\sqrt{5}}{2}$. For any $A < \frac{1}{\sqrt{5}}$, there are finitely many rational solutions $\frac{p}{q}$ to

$$\left|\frac{p}{q} - \beta\right| < \frac{A}{q^2}.$$

(49) If $\beta \neq \frac{-1+\sqrt{5}}{2}$, can you improve (47)?

(50) Suppose β is irrational but not a quadratic irrational (this implies, in particular, it is not periodic). For any $\epsilon > 0$, there exists infinitely many rational $\frac{p}{q}$ such that

$$\left|\frac{p}{q} - \beta\right| < \frac{\epsilon}{q^2}.$$

(51) For some values of d (square-free and positive) the Pell-like equation $x^2 - dy^2 = r$ has non-trivial solutions iff $x^2 - dy^2 = -r$ has non-trivial solutions as long as r is small compared to d. Investigate how small r must be compared to d for this to hold, and find a criteria on $\sqrt{d}$ which predicts when this happens.

(52) Let p be a prime. Consider fractions of the form $\frac{p}{q}$ where $2 \leq q \leq \frac{p-1}{2}$. If the continued fraction expansion is $[a_0, a_1, \ldots, a_n]$, the fraction $[a_n, a_{n-1}, \ldots, a_0]$ obtained by reversing the order is of the same form. If $p \equiv 1 \mod 4$, can it be the same?

Suppose $\frac{p}{q} = [a_0, a_1, \ldots, a_n]$ where $a_i = a_{n-i}$ for all i. Let the convergents be denoted by $\frac{c_k}{d_k}$ to avoid conflicting notation. Show that p divides $c_{n-1}^2 + (-1)^{n-1}$ and so n is odd.

Finally show that

$$p = c_{(n-1)/2}^2 + c_{(n-3)/2}^2.$$

What does this say about when a number is a sum of squares? How efficiently is this computationally?

Hint: If you define

$$\{b_0, b_1, \ldots, b_k\} = b_k\{b_0, b_1, \ldots, b_{k-1}\} + \{b_0, b_1, \ldots, b_{k-2}\},$$

$\{b_0, b_1\} = b_0b_1 + 1$ and $\{b_0\} = b_0$, show that $c_k = \{a_0, a_1, \ldots, a_k\}$ and $d_k = \{a_1, \ldots, a_k\}$. Check that

$$\{b_0, b_1, \ldots, b_n\} = \{b_0, b_1, \ldots, b_m\}\{b_{m+1}, \ldots, b_n\} + \{b_0, \ldots, b_{m-1}\}\{b_{m+2}, \ldots, b_n\}.$$

(53) Although no one knows how to break RSA encryption in general, special cases can be broken. For example, if the decryption key is too small you can find it using continued fractions.

Suppose Bob picks two large primes p and q that satisfy $p < q < 2p$, and let $n = pq$. He picks encryption and decryption keys e, d such that $1 \leq e, d \leq \phi(n)$ and so that $ed \equiv 1 \mod \phi(n)$. e and n are public information, but p, q and d are secret. If by chance $3d < n^{\frac{1}{4}}$, an adversary using knowledge of e and n can find d. Let $k = \frac{ed-1}{\phi(n)}$. Show that

$$\left| \frac{e}{n} - \frac{k}{d} \right| < \frac{1}{3d^2}.$$

Use this to show how to calculate the decryption key using only e and n.

(54) The continued fraction for e begins

$$[1, 0, 1, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, \ldots].$$

Any conjectures? Define the following three integrals

$$\begin{aligned} A_n &:= \int_0^1 \frac{x^n(x-1)^n}{n!} e^x dx \\ B_n &:= \int_0^1 \frac{x^{n+1}(x-1)^n}{n!} e^x dx \\ C_n &:= \int_0^1 \frac{x^n(x-1)^{n+1}}{n!} e^x dx \end{aligned}$$

and show they satisfy the recurrences

$$\begin{aligned} A_n &= -B_{n-1} - C_{n-1} \\ B_n &= -2nA_n + C_{n-1} \\ C_n &= B_n - A_n. \end{aligned}$$

Find the proposed numerator and denominator for convergents in these quantities, and prove it. (Hint: Evaluate them in the form $p + q \cdot e$.)

What happens to these quantities as n goes to infinity?

Now that this works, figure out where these integrals come from. A starting place is the theory of Padé approximants, studied extensively by Hermite's students Padé but first appearing in Hermite's work. The idea is to pick a rational function $\frac{p(z)}{q(z)}$ with the degree of p and q less than or equal to m and n such that

$$\frac{p(z)}{q(z)} = e^z + O(z^{m+n+1}).$$

Then let $z = 1$. To find these approximants, the key idea is to reformulate this definition as requiring that the function

$$z \to \frac{q(z)e^z - p(z)}{z^{m+n+1}}$$

is holomorphic at 0, and that to check whether a function is holomorphic we can just represent it as an integral. If you've computed lots of integrals, you might remember that integrals like

$$\int_0^1 r(x) e^{zx} dx$$

almost have the correct form if $r(x)$ is a polynomial of degree at most $m+n$. Think about what to pick for $r(x)$ by finding a formula for the coefficients of p and q in terms of the derivatives of $r(x)$.

10. Miscellaneous

(55) The goal of this problem is to show that the integers are the unique object satisfying the axioms for $\mathbb{Z}$ (a commutative ring with identity that is totally ordered and such that any non-empty subset of the positive numbers has a least element).

Remember that a ring homomorphism is a map $\phi : R \to S$ such that $\phi(x+y) = \phi(x) + \phi(y)$, $\phi(xy) = \phi(x)\phi(y)$, and $\phi(1) = 1$.

(a) Find a ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_m$. From $\mathbb{Z}$ to $\mathbb{C}$? From $\mathbb{Z}$ to $\mathbb{Q}(\sqrt{2})$? When do these extend to a homomorphism from $\mathbb{Q}$? Conjectures?

(b) Prove that there exists a canonical ring homomorphism from $\mathbb{Z}$ to R, when R is any ring (commutative with identity). In the language of category theory, this means $\mathbb{Z}$ is the initial object in the category of commutative rings with multiplicative identities.
A total ordering is on a set S is a relation $\leq$ such that for any $a, b \in S$ $a \leq b$ or $b \leq a$. Furthermore, $a \leq b$ and $b \leq c$ imply $a \leq c$. $a \leq b$ and $b \leq a$ imply that $a = b$.

(c) Formulate what it means for a total ordering to be compatible with a ring structure. Show that $\mathbb{Z}$ is totally ordered as a ring. Make sure that $\mathbb{Z}_n$ is not totally ordered as a ring.
Now let R be any nontrivial-ring that has a total ordering $\leq$ compatible with the ring structure. Furthermore, assume that $\{r \in R : 0 < r\}$ is well-ordered with respect to $\leq$.
Now consider the canonical map $\phi : \mathbb{Z} \to R$ from 55b.

(d) Show that ϕ is a bijection. Conclude that $\mathbb{Z}$ is unique.

(56) PODASIP: If 2 is a generator for $(\mathbb{Z}/p\mathbb{Z})^{\times}$, then 2 is a generator for $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^{\times}$. The same statement for 10.

(57) Prove Wilson's theorem with a combinatorial argument. One such method starts by counting the number of arrangements of the numbers $0, 1, \ldots, p-1$ in a circle (rotation produces equivalent arrangements, of course). Then consider acting on such arrangements by adding n to each number (modulo p, of course) and group into orbits.

(58) Combinatorially prove that $\binom{ap+b}{cp+d} = \binom{a}{c} \cdot \binom{b}{d} \mod p$ if $0 \leq a, b, c, d < p$. Do this by considering picking $cp + d$ points from an arrangement of p rows of a points with b points left over. Then consider acting on such choices by cyclically shifting the pa points in the rows. Group into orbits to establish the congruence. Can you generalize this?

(59) Find all integer solutions to the equation $x^5 - 1 = \frac{y^7-1}{y-1}$.

(60) Find a formula for the area of simply connected polygon whose vertices are lattice points (in the plane) in terms of the number of lattice points in the interior and on the boundary. Does this work for $\mathbb{Z}^2$ or for any lattice? This is known as Pick's theorem.

(61) Investigate Farey sequences. Geometry may help: you can represent $\frac{a}{b}$ as the lattice point (b, a) in the first quadrant. Given two adjacent terms in a Farey sequence, how close together are they? Also, if $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive terms in a Farey sequence of order n, find the first term that appears between them in a Farey sequence of higher order.

(62) Use your analysis of the Farey sequence to show that, for any irrational α, there exist infinitely many $\frac{p}{q}$ with

$$|\alpha - \frac{p}{q}| \leq \frac{1}{\sqrt{5}q^2}.$$