Math 115 - Introduction to Number Theory

Albert Ye

November 27, 2023

1 Lecture 1

Definition 1

An integer $p \neq 0, 1, -1$ is **prime** if the only integers which divide p are ± 1 and $\pm p$.

Recall that the integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

Theorem 2 (Twin Prime Conjecture)

There are infinitely many $p \in \mathbb{N}$ such that p is prime and $p + 2$ is prime.

Yitang Zhang proved bounded gaps between primes, so there are infinitely many prime $p, p + N$.

Theorem 3 (Goldbach Conjecture)

Every even number can be written as the sum of two primes.

Vinagradar proved that every odd number can be written as the sum of 3 primes. The proof should use something called sieves.

Proposition 4

There are infinitely many primes.

Proof. Suppose not and $p_1, \ldots, p_n$ are all the primes. Then, let $p_1 \cdots p_n + 1 = N$.

As we will see, every integer admits a unique decomposition into a product of primes. □

1.1 Counting Primes

Let $\pi(x) : N \to \mathbb{N}$ return the number of primes p such that $0 < p < x$.

Then, $\pi(x)$ is unbounded: $\lim_{x \to \infty} \pi(x) = \infty$.

Theorem 5 (Prime Number Theorem)

$$\lim \frac{\pi(x)}{x/\log x} = 1.$$

In other words, $\pi(x) \to \frac{x}{\log x}$.

A better approximation is $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$. The error for $\mathrm{Li}(x)$ is $|\pi(x) - \mathrm{Li}(x)| = O(\log x \sqrt{x})$.

1.2 Prime Factorization

Theorem 6 (Uniqueness of Prime Factorization)

Every integer $0 \neq n \in \mathbb{Z}$ can be written as

$$n = (-1)^{Z(n)} \prod_{p \text{ prime}} p^{a_p} \qquad a_p \in \mathbb{N},$$

where all but finitely many a_p are zero, $\epsilon(n) = \begin{cases} 0 & n > 0 \\ 1 & n < 0 \end{cases}$.

To prove this, we first look at a lemma:

Lemma 1.2.1

If $a, b \in \mathbb{Z}$ and $b > 0$, there exist integers q, r such that $a = qb + r$ and $0 \leq r < b$.

Proof. Consider the set of integers of the form $\{a - xb | x \in \mathbb{Z}\} = S$. The set S contains infinitely many positive integers, so contains a least positive integer $r = a - qb$.

Remark 7

This property does not hold for $S \subset \mathbb{Q}$. Consider $S = \{1, \frac{1}{2}, \frac{1}{4}, \ldots\}$.

□

The rest of the proof will follow later.

Definition 8

Let $a_1, \ldots, a_n$ be integers. Denote $(a_1, \ldots, a_n)$ to be the set $\{b_1 a_1 + \cdots + b_n a_n | b_i \in \mathbb{Z}\}$.

2 Lecture 2

2.1 Prime Factorization, cont.

Recall the theorem of uniqueness of prime factorizations. Also recall that a prime number p is an integer $\neq 0$, so that the only divisors of p are ± 1 and $\pm p$.

Definition 9

If $0 \neq a \in \mathbb{Z}$ and $p \in \mathbb{Z}$ is prime, let $\text{ord}_p a$ denote the largest integer n such that $p^n | a$, i.e. $a = p^n b$.

We define $\text{ord}_p 0 = \infty$.

Lemma 2.1.1

If $a, b \in \mathbb{Z}$, then there exists $d \in \mathbb{Z}$ such that $(d) = (a, b)$. Recall Definition 8 for $(a_1, a_2, \ldots, a_n)$.

Proof. Let d be the smallest integer > 0 in (a, b). We claim that $(d) = (a, b)$. As $d \in (a, b)$, we see that $(d) \subseteq (a, b)$. We have to show that $(a, b) \subseteq (d)$.

Take $c \in (a, b)$, then we see from 1.2.1 that $c = qd + r$ with $0 \leq r < d$. THen $r = c - qd \in (a, b)$. By minimality of d, we see that $r = 0$, so $c = qd$ implie $c \in (d)$. □

Definition 10

If $a, b \in \mathbb{Z}$, then a greatest common divisor d of a, b is an integer which divides a, b such that any other integer c with that property satisfies $c|d$.

Remark 11

If we insist $d \geq 0$, then it is unique. Because if $c, d \geq 0$ are both $\gcd(a, b)$, then $c|d$ and $d|c$, which implies $c = \pm d$, but because of positivity we must have $c = d$.

Proposition 12

If $a, b \in \mathbb{Z}$, then the d appearing in 2.1.1 s.t. $d = (a, b)$ is a greatest common divisor of a, b.

Proof. If $(d) = (a, b)$, then $a \in (d) = d\mathbb{Z} \implies d|a$. If $c \in \mathbb{Z}$ is any common divisor of a and b, then c divides $an + bm$ for all $m, n \in \mathbb{Z}$. As $d \in (a, b)$, d has this form, so $c|d$.

Thus, by definition, d must be the greatest common divisor. □

Definition 13

We say that $a, b \in \mathbb{Z}$ are **relatively prime** if $(a, b) = 1$.

In other words, the only nonzero integers that divide a and b are ± 1.

Lemma 2.1.2

Suppose $a|bc$, and $(a, b) = 1$. Then, $a|c$.

Proof. $(a, b) = 1$ implies $1 = an + bm$ for some n, m. So $c = acn + bcm$. Notice that the right term contains bc and the left term contains a, so c must be divisible by a. □

Corollary 14

If p is prime and $p|ab$, then $p|a$ or $p|b$.

Proof. If $(p, a) = p$, then we're done as $p|a$.

Suppose instead that $(p, a) = 1$. From 2.1.2, we have $p|b$. □

We take the contrapositive to see that if a prime p doesn't divide a or b, then it doesn't divide ab.

Proposition 15

Fix a prime p. If $a, b \in \mathbb{Z}$, then $\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b$.

Proof. Let $\operatorname{ord}_p a = n, \operatorname{ord}_p b = m$. Then, we see that $a = p^n c, b = p^m d$ where $p \not| c, p \not| d$. So $ab = p^n c \cdot p^m d = p^{n+m}(cd)$. We know that p cannot divide cd from 14, so $\operatorname{ord}_p ab = n + m$. □

Now, we can finally prove Theorem 6.

Proof of 6. Fix $n \in \mathbb{Z}$ and suppose that $n = (-1)^{\epsilon(n)} \prod_p p^{a_p}$.

Then, fix a prime q. We see that

$$\operatorname{ord}_q n = 0 + \sum_p a_p \operatorname{ord}_q p = a_q.$$

This is because $\operatorname{ord}_q p = \begin{cases} 1 & q = p \\ 0 & q \neq p \end{cases}$. This implies that the only factors that will contribute to $\operatorname{ord}_q n$ are the terms of q, of which there are a_q.

Hence, a_p for each prime p is determined solely by n, so the prime factorization is unique. □

3 Lecture 3

Lemma 3.0.1

Every nonconstant irreducible polynomial has a factorization into nonconstant irreducible polynomials.

4 Lecture 4

4.1 Factorization of Polynomials

Recall 3.0.1 from last lecture.

Again let $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Definition 16

A nonzero polynomial is called **monic** if the coefficient of its leading term is 1.

Definition 17

If $p(x) \in k[x]$ is nonconstant irreducible, and $0 \neq q(x) \in k[x]$ is any other polynomial. Let $\operatorname{ord}_p q$ be defined as the greatest integer $n \geq 0$ such that $p^n(x) | g(x)$ but $p^{n+1}(x) \nmid g(x)$.

Theorem 18

Every nonconstant polynomial $g(x)$ admits a unique factorization of the form $g(x) = c \prod_{p(x)} p(x)^{a_p}$, where $c \in k^x = k \setminus \{0\}$ and the product is over all irreducible, nonconstant, monic polynomials.

Then, $a_p = \operatorname{ord}_p g$, and c is the leading term of g.

We start with the following lemma:

Lemma 4.1.1

If $f(x), g(x) \in k[x]$ are polynomials with $0 \neq g(x)$ then we can find polynomials $q(x)$ and $r(x)$ with either $r(x) = 0$ or $0 \leq \deg r(x) < \deg g(x)$ s.t. $f(x) = q(x)g(x) + r(x)$.

Proof. If $g | f$, then $g(x)q(x) = f(x)$ for some $q(x)$, and let $r(x) = 0$. Suppose otherwise, and $f \neq 0$. Consider the set $f(x) \in \{f(x) - h(x)g(x), h(x) \in k[x]\}$, and let $q(x)$ be such that $r(x) = f(x) - q(x)g(x)$ is of least degree in this set.

It remains to show $r = 0$ or $\deg r < \deg g$. Suppose otherwise, and that $r(x)$ has leading term ax^d and $g(x)$ has leading term bx^n with $d \geq n$. Let $m9x) = \frac{a}{b}x^{d-n}g(x)$. Then $m(x)$ is a polynomial such that $\deg(r(x) - m(x)) < \deg r(x)$.

However, $r(x) - m(x) = f(x) - (q(x) + \frac{a}{b}x^{d-n})g(x)$, so $r(x) - m(x) \in S$. This contradicts the definitions of $r(x)$. □

Definition 19

If $f_1(x), \ldots, f_n(x)$ are polynomials, let $(f_1, f_2, \ldots, f_n)$ be defined similarly to integers.

Lemma 4.1.2

Given $f(x), g(x) \in k(x)$, there is a $d(x) \in k[x]$ s.t. $(f, g) = (d)$.

Proof. Let $d(x)$ be a polynomial of least degree in (f, g). We have $(d) \subset (f, g)$. Let $c(x) \in (f, g)$. Then, if $d|c$, we're done. If not, then there exists $q(x), r(x)$ s.t. $c(x) = q(x)d(x) + r(x)$, with $\deg r(x) < \deg d(x)$. Then $r(x) = c(x) - q(x)d(x) \in (f, g)$, which is a contradiction as $\deg r < \deg d$. □

5 Lecture 5

Continue proving 18.

Definition 20

We say $f(x), g(x) \in k[x]$ are **relatively prime** if $(f, g) = 1$.

Definition 21

A greatest common divisor, or gcd of f and $g \in k[x]$ is a polynomial $d(x)$ which divides f and g and has the property that if $c(x) \in k[x]$ divides f and g then $c|d$. (Ambiguous up to a scalar.)

Lemma 5.0.1

If f and g are relatively prime and $f|gh$, then $f|h$.

Proof. If $(f, g) = 1$ then $1 = a(x)f(x) + b(x)g(x)$. So $h(x) = a(x)f(x)h(x) + b(x)g(x)h(x) = f(x)(a(x)h(x) + b(x)j(x))$ for some other polynomial $j(x)$. Then, $f(x)|h(x)$. □

If $d(x) = (f(x), g(x))$ and $x \in k^x$ then αd is also a gcd o f and g; $(\alpha d) = (d)$.

Now, recall that a nonconstant polynomial $f(x)$ is **irreducible** if its only divisors are of the form αf or α ($\alpha \in k^*$); i.e. if any polynomial divides f, it's either a scalar or a scalar multiple of f.

Lemma 5.0.2

If $p(x)$ is irreducible and $p|fg$, then $p|f$ or $p|g$.

Proof. $(p, f) = (1)$ or $(p) = (\alpha p)$ for all $x \in k^*$. If $(p, f) = (p)$, then $p|f$. Otherwise, $(p, f) = (1)$, so from Lemma 5.0.1 we have $p|g$. □

Definition 22 (Order in Polynomial Terms)

If p is a nonconstant polynomial and $g \neq f \in k[x]$ then $\operatorname{ord}_p f$ is the largest $a \in \mathbb{Z}_{\geq 0}$ such that $p^a|f$.

Lemma 5.0.3

If $p(x) \in k[x]$ is irreducible and $a, b \in k[x]$, then $\operatorname{ord}_p(ab) = \operatorname{ord}_p(a) + \operatorname{ord}_p(b)$.

Finally, we can prove 18.

Proof. Weite $0 \neq f(x) = c\prod_p p(x)^{a_p}$. For every monic irreducible polynomial q, $\operatorname{ord}_q f = \sum_f a_p \operatorname{ord}_q p$, and we see that $\operatorname{ord}_q p = \begin{cases} 1 & q = p \\ 0 & q \neq p. \end{cases}$. This must be a_q.

The scalar c is the leading coefficient of f, so every polynomial factorization uniquely determines one polynomial. □

6 Lecture 6

Proposition 23

If $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (any field) then $k[x]$ contains infinitely many irreducible polynomials.

Proof. Suppose not, and $p_1(x), \dots, p_n(x)$ exhaust the irreducible polynomials. Thus $q(x) = 1 + p_1(x)p_2(x)\cdots p_n(x)$ is a polynomial not divisible by the $p_i(x)$, but it must factor into a product of the $p_i(x)$, a contradiction. □

Lemma 6.0.1

Every integer $n \neq 0$ can be written as $n = ab^2$ where a is squarefree.

Definition 24

An integer $n \neq 0$ is squarefree if it isn't divisible by the square of any prime.

Proof. If $|n| = 1$ then it's squarefree. If $|n| > 1$ then $n = (-1)^{\epsilon(n)} p_1^{2a_1+b_1} \cdots p_m^{2a_m+b_m}$, where b_i is either 0 or 1 for all i. Then, in turn,

$$n = [p_1^{2a_1} \cdots p_m^{2a_m}][(-1)^{\epsilon(n)} p_1^{b_1} \cdots p_m^{b_m}].$$

We see that the first term is b^2 and the second term is a squarefree a. □

Definition 25

$\nu(n)$ =number of positive divisors

$\sigma(n)$ =sum of positive divisors

Proposition 26

Let $n \in \mathbb{Z}_{>1}$ have a prime factorization $n = p_1^{a_1} \cdots p_m^{a_m}$. Then,

- $\nu(n) = (a_1 + 1)(a_2 + 1) \cdots (a_n + 1)$
- $\sigma(n) = \left(\sum_{i=0}^{a_1} p_1^i\right) \cdots \left(\sum_{i=0}^{a_n} p_n^i\right)$.

Recall that $\sum_{n=a}^{b} x^n = \frac{x^{b+1}-x^a}{x-1}$, so $\sigma(n) = \left(\frac{p_1^{a_1+1}-1}{p_1-1}\right) \cdots \left(\frac{p_n^{a_n+1}-1}{p_n-1}\right)$.

Definition 27

An integer > 0 is **perfect** if $\sigma(n) = 2n$.

Euler claimed that every even perfect number can be written as $2^m(2^{m+1} - 1)$, where $2^{m+1} - 1$ is a Mersenne prime.

6.1 Mobius Function

Definition 28 (Mobius Mu Function)

The Mobius $\mu : Z_{>0} \to \{0, \pm 1\}$ returns $\mu(n) = 0$ if n is not squarefree, $\mu(1) = 1$, and if $n > 1$, $n = p_1, \dots, p_m$, then $\mu(n) = (-1)^m$.

Proposition 29

If $n > 1$ then $\sum_{d|n} \mu(d) = 0$.

Proof. $n = p_1^{a_1} \cdots p_m^{a_m}$. Notice that for any $a_i > 1$, we can ignore and take mod 2 because non-squarefree implies a Mobius of 0.

Therefore, $\sum_{d|n} \mu(d) = \sum \mu(p_1^{\epsilon_1} \cdots p_m^{\epsilon_m}) = (1-1)^m = 0$. □

6.2 Dirichlet Convolution

Definition 30

If f, g are two functions $\mathbb{Z}_{>0} \to \mathbb{C}$, then the Dirichlet convolution of f and g is defined to be $(f \cdot g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$.

Remark 31

Dirichlet convolution is associative; given $f, g, h : \mathbb{Z}_{>0} \to \mathbb{C}$, then $((f \cdot g) \cdot h)(n) = (f \cdot (g \cdot h))(n) = \sum f(d_1)g(d_2)h(d_3)$,

Definition 32

Let $1(n) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$. Then, $(f * 1)(N) = \sum_{d|n} f(d)$.

Theorem 33 (Mobius Inversion)

If $f : \mathbb{Z}_{>0} \to \mathbb{C}$ and $F(n) = \sum_{d|n) f(d)}$, then $\sum_{d|n} F(d)\mu\left(\frac{n}{d}\right) = f(n)$, or as we simplify it, $\mu \times F = f$.

7 Lecture 7

7.1 Prime Counting

Definition 34 (Euler Totient)

We define $\phi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$. $\phi(n)$ is the number of integers in $[1, n]$ relatively prime to n.

$\phi(1) = 1$, $\phi(p) = p - 1$ for prime p.

Proposition 35

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

Proof. Consider the set $\left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\right\}$. Write these fractions in lowest terms.

For each $d|n$, we wish to count the functions above with d in lowest terms. These fractions will be a subset of the fractions $\frac{a}{n}$ where $\frac{n}{d}|a$, i.e. a subset of the fractions $\left\{\frac{1}{d}, \frac{2}{d}, \ldots, \frac{d}{d}\right\}$. There are $\phi(d)$ many fractions on this list with d in the domain, when written in lowest terms.

So if $J_d \subset \left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\right\}$ corresponds to the fractions of denominator d in lowest terms, then $S = \bigcup_{d|n} J_d$, and $n = |S| = \sum_{d|n} |J_d| = \sum_{d|n} \phi(d)$. □

From Mobius inversion, we have $\phi = (\phi \cdot 1) \cdot \mu$. We know that $(\phi \cdot 1) = id$ where $id(n) = n$, so we have $\mu \cdot id = \sum_{d|n} \mu(d)\frac{n}{d}$. Now, let $n = p_1^{a_1} \cdots p_m^{a_m}$. Then,

$$\begin{aligned} \mu \cdot id &= n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} \cdots \text{ (by definition of Mobius inversion)} \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right) = \phi(n). \end{aligned}$$

Theorem 36

$\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

Also consider $\pi(x) = \frac{x}{\log x}(1 + \left(\frac{1}{\log x}\right)$.

Proof. Of $n \in \mathbb{Z}_{>0}$, let $p_1, \ldots, p_{\pi(n)}$ be the primes $\leq n$ and let

$$\lambda(n) = \prod_{i=1}^{\pi(n)} \left(1 - \frac{1}{p_i}\right)^{-1}.$$

Notice that each inner value for the product term is $\sum_{a=0}^{\infty} \left(\frac{1}{p_i}\right)^a$.

Then, $\lambda(n) = \sum \frac{1}{p_1^{a_1} \cdots p_{\pi(n)}^{a}}$, where the sum is over all $\pi(n)$-tuples $(a_1, \ldots, a_{\pi(n)}) \in \mathbb{Z}_{\geq 0}^{\pi(n)}$. Then, we have

$$\log \lambda(n) = -\sum_{i=1}^{\pi(n)} \log(1 - p_i)^{-1} = \sum_{i=1}^{\pi(n)} \sum_{m=1}^{\infty} (m p_i^m)^{-1}.$$

If we can prove that $\log \lambda(n)$ converges, then we see that $\lambda(n)$ is divergent and we are done.

I'll pick this up later.

Somehow we're done. Easy. □

8 Lecture 8

We go back to 36. Because of a fire alarm, there wasn't anything else covered.

9 Lecture 9

9.1 Estimates for Prime Counting Function

Last time, we proved that $\sum_p \frac{1}{p}$ for prime p diverges.

We go back to 5, the Prime Number Theorem.

Theorem (Prime Number Theorem)

$$\pi(x) = \frac{x}{\log x}\left(1 + O\left(\frac{1}{\log x}\right)\right).$$

Theorem 37

$$\sum_{p \text{ prime}, p \leq n} \frac{1}{p} = \log \log n + C.$$

Proof. Sketch: We turn p into a function of $\pi(x)$, and then use $\pi(n)$ □

We let $\theta(x) = \sum_{p \leq x, p \text{ prime}} \log p$.

10 Lecture 10

10.1 Estimates for Prime Counting Function

Lemma 10.1.1

$\theta(x) = \sum_{p \le x, p \text{ prime}} \log p < (4 \log 2)x$.

Proposition 38

There exists a constant $C_2 \in \mathbb{R}_{>0}$ such that $\pi(x) < \frac{c_2 x}{\log x}$.

Proof.

$$\begin{aligned}
\theta(x) &= \sum_{p \le x, p \text{ prime}} \log p \\
&> \sum_{p \ge \sqrt{x}, p \text{ prime}}^{p \le x} \log p \\
&\ge \log \sqrt{x}(\pi(x) - \pi(\sqrt{x})) \\
&= \log \sqrt{x}\pi(x) - \sqrt{x} \log \sqrt{x}. \\
\pi(x) &\le \frac{2\theta(x)}{\log x} + \sqrt{x} \\
&< (8 \log 2)\frac{x}{\log x} + \sqrt{x} \\
&< (2 + 8 \log 2)\frac{x}{\log x} < \frac{2x}{\log x}.
\end{aligned}$$

Therefore, we see that $c_2 \ge 2$ works. □

Proposition 39

There exists a constant $c_1 \in \mathbb{R} \ge 0$ such that $\frac{c_1 x}{\log x} < \pi(x)$.

Proof. $\theta(x) \sim \binom{2n}{n} = \left(\frac{n+1}{1}\right)\left(\frac{n+2}{2}\right) \cdots \left(\frac{2n}{n}\right) \ge 2^n$.

Let $t_p = \lfloor \frac{\log 2n}{\log p} \rfloor = \log_p 2n$. We also see that $n \log 2 \le \sum_{p \le n, p \text{ prime}} t_p \log p = \sum_{p \le n, p \text{ prime}} \lfloor \frac{\log 2n}{\log p} \rfloor \log p = K$.

If $\log p > \frac{1}{2}\log(2n)$, then $\frac{\log 2n}{\log p} < 2$ and its floor is 1.

Then, $K = \sum_{p \text{ prime}, p \le \sqrt{2n}} \lfloor \frac{\log 2n}{\log p} \rfloor \log p + \sum_{p \text{ prime}, 2n > p > \sqrt{2n}} \log p \le \theta(2n)$.

Putting in $n \log 2 \le K$, we have $n \log 2 \le \sqrt{2n} \log 2n + \theta(2n)$, so $\theta(2n) \ge n \log 2 - \sqrt{2n} \log 2n$.

Next time, we'll show that this estimate for θ implies a lower bound for $\pi(x)$. □

11 Lecture 11

11.1 Announcements

Brief summary of topics covered:

1.1, 1.2, entirety of Chapter 2, 3.1, 3.2. The hardest parts are also not easy to test, and should not be memorized. Because that would be absolutely fucking evil.

11.2 Estimates for Prime Counting Function

Last time, we were trying to prove:

Theorem 40

$$\pi(x) < \frac{c_2}{\log x},$$

for some constant $c_2 \in \mathbb{R}$.

11.3 Congruence

We define $a \equiv b \pmod{n}$ to mean that $n|(a-b)$.

Definition 41

The relation of congruence defines an **equivalence relation** aRb. An equivalence relation is a relation which is revlexive, symmetric, and transitive.

- $a \equiv a$
- $a \equiv b \implies b \equiv a$
- $a \equiv b, b \equiv c \implies a \equiv c$.

Given a set S and an equivalence relation R, on S we can form the set $[x] = \{y \in S | yRx\}$.

In our case, $a \in \mathbb{Z} \implies \overline{a} := [a] = \{b \in \mathbb{Z} | a \equiv b \pmod{n}\}$.

Definition 42

If $a \in \mathbb{Z}$, $\overline{a} = \{a + nb | b \in \mathbb{Z}\}$ is called the **congruence class** of a for the modulus n.

Proposition 43

The equivalence classes for R on S partition S.

That is, every $x \in S$ is in some equivalence class ($x \in [k]$), and given $x, y \in S$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.

Proof. If $z \in [x] \cap [y]$, xRz and zRy so xRy, so any $w \in S$ has the property that $wRx = wRy \implies [x] = [y]$. □

For congruence, this boils down to the fact that

- $\overline{a} = \overline{b} \iff a \equiv b \pmod{n}$.
- $\overline{a} \neq b \iff \overline{a} \cap \overline{b} = \emptyset$
- There are precisely n congreunce classes modulo n.

12 Lecture 12

12.1 Equivalence Classes, Continued

The set of equivalence classes modulo n is defined as $\mathbb{Z}/n\mathbb{Z}$.

Lemma 12.1.1

The set $\mathbb{Z}/n\mathbb{Z}$ admits addition and multiplication by the formulas:

- $\overline{a} + \overline{b} = \overline{a+b}$.
- $\overline{a} \cdot \overline{b} = \overline{ab}$.

Proof. To check that $+$ and $\cdot$ are defined in this way are well-defined, we must show that we'd get the same thing when changing the representatives, i.e., replacing $\overline{a}$ by $a + kn$ for $k \in \mathbb{Z}$.

$$\overline{a+kn+b+jn} = \overline{a+b} \implies a+kn+b+jn \equiv a+b \pmod{n},$$

which is true after removing all obvious multiples of n. The proof for $\overline{ab}$ is too long to fit in the margins, but it works similarly. □

An application of this is finding which polynomials in $\mathbb{Z}[x]$ have no integer solutions.

Remark 44

If $a \equiv b \pmod{n}$, then $a^m \equiv b^m \pmod{n}$.

Let $p(x) = c_m x^m + \cdots + c_1 x + c_0$ for integer c_i. If $a \equiv b \pmod{n}$, we further see that $p(\overline{a}) := \overline{p(a)}$ must equal $p(\overline{b})$. Therefore, $c_m a^m \equiv c_m b^m \pmod{n}$, so $\overline{c_m} a^m = \overline{c_m} b^m$.

Now, we suppose $n = 2$. Then, $p(0) = c_0$, $p(1) = c_n + c_{n-1} + \cdots + c_0$. If $p(x)$ has a solution in the integers, then it must have a solution mod 2 ($p(k) = 0 \implies p(\overline{k})\overline{0}$. So, any $p(x) \in k[x]$ with integer solutions must have $p(\overline{0}) = \overline{0}$ or $p(\overline{1}) = \overline{1}$.

Proposition 45

Any $p(x)$ with c_0 odd and $\sum_{i=0}^{n} c_i$ odd has no integer solutions.

Now, for the general criterion modulo n:

Theorem 46

If $c_0 \not\equiv 0 \pmod{n}$, and $\sum_{i=0}^{m} k^i c_i \not\equiv 0 \pmod{n}$ for all $0 < k < n$, then $p(x)$ has no integer solutions.

13 Lecture 13

13.1 Announcements

Topics of the test: same as in 11.1.

Need to know the facts about divergence $\sum_p \frac{1}{p}$, $\frac{c_1 x}{\log x} < \pi(x) < \frac{c_2 x}{\log x}$, but don't need to remember the whole proofs for all of them.

Also there is another book with a lot of review problems: Niven, Montgomery, and Zuckerman, *An Introdution to the Theory of Numbers*, 5e. §1.2, §1.3, §4.2, §4.3 are good practice. If not much time, because of tests like the 126 midterm, just review and understand solutions for the questions assigned.

13.2 Diophantine Equations

We're looking for solutions to $ax \equiv b \pmod{m}$. Because if x_0 solves $ax_0 \equiv b \pmod{m}$, then so does $x_0 + km$.

Lemma 13.2.1

Let $d := (a, m)$ and let $a' = \frac{a}{d}$, $m' = \frac{m}{d}$. The equation $ax \equiv b \pmod{m}$ admits a solution iff $d|b$.

If $d|b$ then there are exactly d solutions.

If x_0 is a solution, tnen $x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'$ is a list of all solutions to $ax \equiv b \pmod{m}$.

Proof. For the first claim: suppose we've found a solution x_0 to $ax \equiv b \pmod{m}$, i.e. $m|(ax_0 - b)$. So, $ax_0 = b \equiv km$ for source $k \in \mathbb{Z}$. As $d|a$ and $d|m$, $d|b$. Conversely, if $d|b$, then set $c = \frac{d}{b}$. Because $d = (a, m)$ we can find $x_0', y_0' \in \mathbb{Z}$ such that $ax_0' + my_0' = d$. Multiplying by c, we have $cax_0' + cmy_0' = b$, so $x_0 = cx_0'$ solves $ax_0 \equiv b \pmod{m}$. □

For the second claim: suppose x_0 and x_1 both solve $ax \equiv b \pmod{m}$. So, $ax_0 - b = k_1 m$ and $ax_1 - b \equiv k_2 m$. Then, this means that $a(x_0 - x_1) \equiv 0 \pmod{m}$. $d = (a, m)$, so $m|a(x_0 - x_1)$ implies $\frac{m}{d} = m'$ divides $x_0 - x_1$, so $x_1 = x_0 + km'$ for some $k \in \mathbb{Z}$.

Ifx_0 solves $ax \equiv b \pmod{m}$, then $x_0 + km'$ does too for every $k \in \mathbb{Z}$. akm' is divisible by m so they must be $\equiv 0 \pmod{m}$, so $ax_0 \equiv a(x_0 + km') \pmod{m}$.

We claim that $x, y \in x_0, x_0 + m', \ldots, x_0 + (d-1)m'$ are inequivalent modulo m, which follows as $(x_0 + k_1 m') - (x_0 + k_2 m') = (k_1 - k_2)m'$ and $0 < k_1 - k_2 < d$, since $0 \leq k2 < k_1 < d$. Therefore, this is not equivalent to 0 modulo m. □

For our third claim: if $x_0 + km'$ is any solution to $ax \equiv b \pmod{m}$, hen $k \equiv k' \pmod{d}$ for some $k' \in [0, d)$. Then, we have $km' \equiv k'm' \pmod{m}$, so $x_0 + km' \equiv x_0 + k'm' \pmod{m}$. □

Corollary 47

if $(a, m) = 1$, the equation $ax \equiv b \pmod{m}$ has exactly one solution.

Corollary 48

If $m = p$ is prime, then $ax \equiv b \pmod{p}$ has only one solution provide $p \nmid a$.

Remark 49

If m is not prime, then $m = m_1 m_2$ with $0 < m_1, m_2 < m$ so $m_1 m_2 \equiv 0 \pmod{m}$. So in $\mathbb{Z}/m\mathbb{Z}$, $\overline{m_1} \neq 0 \neq \overline{m_2}$ but $\overline{m_1 m_2} = 0$. Then, $\overline{m}_1$ cannot have an inverse $\overline{m_1}^{-1}$ because then $\overline{m_2} = \overline{m_1}^{-1}\overline{m_1 m_2} = \overline{m_1}^{-1}\overline{0} = 0$.

14 Lecture 14

14.1 Inverse

The main question for today is when $a \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse.

Theorem 50 (Euler's Theorem)

if $m > 1$ is an integer an $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

We also have a corollary:

Corollary 51

If p is prime and p doesn't divide a, then $a^{p-1} \equiv 1 \pmod{p}$.

This corollary is Fermat's little theorem.

Proof. Form the set S of units in $\mathbb{Z}/m\mathbb{Z}$. $|S| = \phi(m)$ and $a \in S$ as $(a, m) = 1$. We claim that $s = \{as | s \in S\}$.

We see that S is bijective to S, so we see that S is bijective to aS, as a is relatively prime to m. We see that

$$\prod_{s \in S} s = \prod_{s \in S} as = a^{|S|} a^{\phi(m)} \prod_{s \in S} s.$$

Taking the inverse, we see that $a^{\phi(m)} \equiv 1 \pmod{m}$. □

14.2 Chinese Remainder Theorem

Theorem 52 (Chinese Remainder Theorem)

Suppose that $m = m_1, \ldots, m_t$ and that $(m_i, m_j) = 1$. For all $1 \leq i < j \leq t$, let $b_1, \ldots, b_t \in \mathbb{Z}$ and consider the system of congruences

$$\begin{aligned} x &\equiv b_1 \pmod{m_1}, \\ x &\equiv b_2 \pmod{m_2}, \\ &\cdots \\ x &\equiv b_t \pmod{m_t}. \end{aligned}$$

This system has a solution and any two solutions differ by a multiple of m.

That is, any system of congruences centered around x must have a unique x modulo m, where m is the product of all moduli in the system, and all moduli in the system are coprime.

Lemma 14.2.1

If $m \in \mathbb{Z}$ and $a_1, \ldots, a_t$ are each relatively prime to m, then $a - 1, \ldots, a_t$ is.

Lemma 14.2.2

If $a_1, \ldots, a_t$ divide $n \in \mathbb{Z}$ and $(a_i, a_j) = 1$ for $1 \leq i < j \leq t$, then $a_1 \cdots a_t | n$.

Proof. The integers a_i determine a partition of a subset of the prime factors of n, by definition. □

I honestly tuned out the proof of CRT oops

15 Lecture 15

161

16 Lecture 16

16.1 The Primitive Element

Theorem 53 (Primitive Element)
For each prime p, there is an $\alpha \in \mathbb{Z}/p\mathbb{Z}$ s.t. $(\mathbb{Z}/p\mathbb{Z})^* = \{1, \dots, p+1\} = \{\alpha, \alpha^2, \dots, \alpha^{p+1}\}$.

Proposition 54
If $d|p-1$, then $x^d \equiv 1(p)$ has exactly d solutions in $\mathbb{Z}/p\mathbb{Z}$.

We are finally making it into the abstract algebra class with this next one:

Definition 55 (Group)
A **group** is a set S endowed with a binary operation $\cdot$, with the property that $x \cdot y \in S$

1. If $x, y, z \in S$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. *(associativity)*
2. There is an element $e \in S$ s.t. $e \cdot x = x = x \cdot e$ for all $x \in S$. *(identity)*
3. For any $x \in S$ there exists $x^{-1} \in S$ s.t. $x \cdot x^{-1} = e = x^{-1} \cdot x$. *(invertibility)*

Definition 56 (Cyclic Group)
A group is **cyclic** if there exists an element $g \in G$ such that every $x \in G$ equals g^i for some i depending on x.

So, Theorem 53 essentially wants us to prove that $((\mathbb{Z}/p\mathbb{Z}), \times)$ forms a cyclic group!

Definition 57 (Order)
If $x \in G$ and G is a inite group, then the order $\operatorname{ord} x$ of x is the least positive integer such that $x^{\operatorname{ord} x} = e$.

$\operatorname{ord} e = 1, \operatorname{ord} x > 1$ if $x \neq e$.

Lemma 16.1.1
If G is a finite abelian group of order n, then if $x \in G, x^n = e$.

Corollary 58
If G is finite (abelian) and $x \in G$, then $\operatorname{ord} x || G|$.

Proof of Primitive Element. If $d|p-1$, let $\psi(d)$ denote the number of elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of order d. An element $a \in (\mathbb{Z}/p\mathbb{Z})^*$ satisfies $a^d = 1$ if and only if $\operatorname{ord} a | d$ If $d = c \cdot \operatorname{ord} a$, then $a^d = (a^{\operatorname{ord} a})^c = 1^c = 1$. Conversely, if $a^d = 1 \in \mathbb{Z}/p\mathbb{Z}$, then I claim $\operatorname{ord} a | d [a^{(\operatorname{ord} a, d)} = 1$.

From the proposition, we see that $d = \sum_{c|d} \psi(c)$. Taking the Mobius inversion, we get that $psi = \phi$, so there is an element of $(\mathbb{Z}/p\mathbb{Z})$ with order $p-1$. □ □

17 Lecture 17

Reminder that not all n are cyclic; example is $n = 4$.

Theorem 59
If p is an odd prime and $l \in \mathbb{Z}_{>0}$, $(\mathbb{Z}/p^l\mathbb{Z})^*$ possess a primitive element, so it is cyclic.

Lemma 17.0.1

If p is prime and $1 \leq k \leq p$, then $\binom{p}{k}$ is divisible by p.

Proof. $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, and $k < p, p-k < p$ so p does not divide $k!, (p-k)!$. Thus, there must be a factor of p. □

Lemma 17.0.2

If $a \equiv b \pmod{p^l}$, then $a^p \equiv b \pmod{p^{l+1}}$.

Proof. $a = b + cp^l$, so

$$\begin{aligned} a^p &= (b + cp^l)^p \\ &= b^p + \binom{p}{1} b^{p-1} cp^l + A \end{aligned}$$

where $p^{2l} | A$. As $2l \geq l+1$, $a^p \equiv b^p \pmod{p^{l+1}}$. □

Corollary 60

If $l \geq 2$ and $p \neq 2$, then $(1+ap)^{p^{l-1}} \equiv 1 + ap^{l-1} \pmod{p^l}$ for all $a \in \mathbb{Z}$.

Proof. induct on l. If $l = 2$, then $(1+ap)^1 = 1 + ap^1$.

Assume it holds for some $l \geq 2$, we prove it for $l+1$.

$$(1+ap)^{p^{l-1}} = ((1+ap)^{p^{l-2}})^p.$$

From Lemma 2, we have thta this is congruent to $(1+ap^{l-1})^p$ modulo p^{l+1}. And then, $(1+ap^{l-1})^p = 1 + \binom{p}{1} ap^{l-1} + B$, so all the terms in B are divisible by $p^{1+2(l-1)}$, except for the last term $a^p p^{p(l-1)}$.

We'll be done if we can show $p^{l+1} | p^{1+2(l-1)}$ and $p^{l+1} | p^{p(l-1)}$, tha tis, that $1 + 2(l-1) \geq l+1$, and $l+1 \leq p(l-1)$, since $l \geq 2, p > 2$. Therefore, $B \equiv 0 \pmod{p^{l+1}}$. □

Corollary 61

If $p \neq 2$ and $p \not| a \in \mathbb{Z}_{>0}$, then $p^{l-1} \equiv \operatorname{ord}(1+ap) \pmod{p^l}$.

We define $b \in \mathbb{Z}_{>1}$, where $(b, n) = 1$, has order $l \pmod{n}$ if its order in $(\mathbb{Z}/n\mathbb{Z})^*$ is l. Equivalently, l is the least $\mathbb{Z}_{>0}$ such that $b^l \equiv 1 \pmod{n}$.

18 Lecture 18

Started the proof in lec 17, continue in lec 18.

Proof of 59. There exist primitive roots $\pmod{p}$. Pick one, call it $g \in \mathbb{Z}$. Then, $\overline{g} = \overline{g+p}$ so $g+p$ is also a primitive rood modulo p. If $g^{p-1} \equiv 1 \pmod{p^2}$, then $(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2} \cdot p \pmod{p^2}$.

We see that the first term is equivalent to 1. So, if p does not divide g^{p-2}, then the $g^{p-1} + (p-1)g^{p-2} \cdot p \neq 1 \pmod{p^2}$, meaning g is a primitive root mod p.

Now, assume I can find a primitive root modulo p, call it g'. Then, I claim g' is a primitive root mod p^l for any $l > 0$. □

19 Lecture 19

Last time we showed that if m has primitive roots and if $(a,m)=1$, then $x^n \equiv a \pmod m$ has a solution if and only if $a^{\phi(m)/d} \equiv 1 \pmod m$, where $d=(\phi(m),n)$.

Remark 62

If $x^n \equiv a \pmod m$ has a solution (a,m,n) as above, then it has $(n,\phi(m))$ solutions.

Proof. If g is a primitive root for m, x □

In particular, if $m=p$ is prim,e then $x^n \equiv a \pmod p$ has a solution if and only if $a^{(p-1)/d} \equiv d \pmod p$, wherre $d=(p-1,n)$.

If $n=z \neq p$, we have $x^2 \equiv a \pmod p$ has a solution if and only if $a^{(p-1)/z \equiv 1 \pmod p}$.

Lemma 19.0.1

Suppose $m \equiv 2^e p_1^{a_1} \cdots p_l^{a_l}$ if a prime factorization of $m \in \mathbb{Z}_{>0}$ and $(a,m)=1$. Then a is a quadratic residue mod m iff

(a) If $e=2$, then $a \equiv 1 \pmod 4$
If $e \geq 3$, then $a \equiv 1 \pmod 8$.

(b) $a^{(p_i-1)/2} \equiv 1 \pmod{p_i}$ for all i.

Lemma 19.0.2

If p is an odd prime, p not dividing a or n, then if $x^n \equiv a \pmod p$ has a solution, then $x^n \equiv a \pmod{p^e}$ is solvable for every $e \geq 1$. All these congruences have the same number of solutions.

Lemma 19.0.3

Let 2^l be the highest power of 2 which divides n. Suppose a is odd and that $x^n \equiv a \pmod{2^{2l+1}}$ is solvable. Then, $x^2 \equiv a \pmod{2^l}$ is solvable for all $e \geq 1$, and all these congruence equations have the same number of solutions.

20 Lecture 20

unsure. missed it. oops

Definition 63 (Legendre Symbol)

$\frac{a}{p}$ is defined as the Legendre Symbol, which equals:

- 0 if $a \equiv 0 \pmod p$
- 1 if a is another quadratic residue modulo p
- -1 if a is a quadratic nonresidue modulo p.

Lemma 20.0.1 (Gauss's Lemma)

Consider the set of least residues $S=\{-(p-1)/2, -(p-3)/2, \ldots, -1, 1, 2, \ldots, (p-1)/2\}$. Let μ be the number of least residues $a, 2a, \ldots, (p-1)a/2$ that are negative.

Then, $(a/p)=(-1)^\mu$.

21 Lecture 21

21.1 Quadratic Reciprocity

The question we're trying to answer is when primes are squares modulo n.

We introduced a set $S = \{-\frac{p-1}{2}, \dots, -1, 1, \dots, \frac{p-1}{2}\}$, which we call the **set of least residues** modulo p.

If $a \in \mathbb{Z}, p \not| a$, we form $\{a, 2a, \dots, \frac{p-1}{2}a\}$ and we ask how many of this set are negative least residues mod p. Call this number μ.

Lemma 21.1.1 (Gauss' Lemma)

$$(-1)^\mu = (a/p), \text{ where } (p \nmid a).$$

Proof. For each integer $1 \le l \le \frac{p-1}{2}$, let $\pm m_l$ be the least residue corresponding to la, where $m_l > 0$. As l ranges over $1, 2, \dots, \frac{p-1}{2}$, the number of negative signs appearing in the $\pm m_l$ is given by μ.

We claim now that $\left\{m_l | 1 \le l \le \frac{p-1}{2}\right\} = \{1, \dots, (p-1)/2\}$.

We have

$$\prod l = 1^{(p-1)/2} la = (-1)^\mu \prod_{i=1}^{(p-1)/2} i.$$

This then equals

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

Plugging in the Legendre symbol gives us $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod p$. □

Proposition 64

$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p-1}{8}}$.

Proof. In this case $a = 2$, and μ is the number of numbers in the set $2, 2 \cdot 2, 3 \cdot 2, \dots, 2\left(\frac{p-1}{2}\right)$ which are strictly greater than $\frac{p-1}{2}$. Let m be the integer characterized by $2m \le \frac{p-1}{2}$ and $2(m+1) > \frac{p-1}{2}$. So $\mu = \frac{p-1}{2} = k$. So $\mu = \frac{p-1}{2} = m$. □

Corollary 65

Infinitely many primes of the form $8k + 2$.

Proof. Suppose not and $p_1, \dots, p_n$ are all of them. Then, $n = (1 \cdot p_1, \cdot \dots \cdot c_n)^2$, where $\lambda \equiv 0 \pmod n$ and $n \equiv 0 \pmod p$ if $p|n$.

Moreover, Z is also a square modulo any $p|n$. So if $p|n, p \equiv 1, 7 \pmod 8$. Then, $\frac{n}{2} \equiv 7 \pmod 8$. Not all the prime divisors of $\frac{n}{2}$ can be $\equiv 1 \pmod 8$, so there exists a prime $p \nmid n$ such tat $p \equiv 7 \pmod 8$), where $p \neq p_i$.

To be continued... □

Theorem 66 (Quadratic Reciprocity) (a) $(-1/p) = (-1)^{(p-1)/2}$

(b) $(2/p) = (-1)^{(p^2-1)/8}$

(c) $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$.

If one of p or q is $\equiv 1 \pmod 4$, then p is a quadratic residue mod q iff q is a residue mod p.

If both p and q are $\equiv 3 \pmod 4$, then p is a residue iff q is a nonresidue.

This further implies that if either p or q is equivalent to 1 modulo 4, then $(p/q) = (q/p)$. If both are 3 modulo 4, then $(p/q) = -(q/p)$.

22 Lecture 22

Theorem 67 (i) If $q \equiv 1 \pmod 4$ then q is a residue mod p iff $p \equiv r \pmod q$ where r is a quadratic residue mod q.

(ii) If $q \equiv 3 \pmod 4$, then q is a quadratic residue mod p iff $p \equiv \pm b^2 \pmod{4q}$ for some odd integer b prime to q.

Proof. 1. $(q/p) = (p/q)$.

2. If $q \equiv 3 \pmod 4$, then $(q/p) = (-1)^{((p-1)/2)((q-1)/2)}(p/q)$.
   Assume that $p \equiv \pm b^2 \pmod{4q}$ where b is odd and $(b, q) = 1$.
   If $p \equiv b^2 \pmod{4q}$, then $p \equiv b^2 \equiv 1 \pmod 4$, so $(q/p) \equiv (p/q)$, and $p \equiv b^2 \pmod q$ so $(p/q) = 1$. So, $(q/p) = (1)(1) = 1$.
   If $p \equiv -b^2 \pmod{4q}$, then $p \equiv 3 \pmod 4$, so $(q/p) = -(p/q)$. As $p \equiv -b^2 \equiv q$ as well, we see that $(-b^2/q) = (-1/q)(b/q)^2 - 1$. Therefore, $(p/q) = (-b^2/q) = -1$, so $(q/p) = (-1)(-1) = 1$.

□

Example 68

For which primes is $a = 6$ a quadratic residue?

We have

$$(6/p) = (2/p)(3/p) = 1 \iff (2/p) = 1, (3/p) = 1 \text{ or } (2/p) = -1, (3/p) = -1.$$

For the first case, we have $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 1 \pmod{12}$, so $p \equiv \pm 1 \pmod{24}$.

For the second case, we have $p \equiv \pm 3 \pmod 8$ and $p \equiv \pm 5 \pmod{12}$. The first congruence becomes $p \equiv \mp 5 \pmod 8$, so we see once again that both are simultaneously true if $p \equiv \pm 5 \pmod 2)4$.

Therefore, primes p such that $p \equiv \pm 1$ or $p \equiv \pm 5$.

Theorem 69

Suppose a is a nonsquare integer. Then, there are infinitely many primes for which a is a quadratic nonresidue.

Corollary 70

If a is a quadratic residue mod every prime, it is a square.

23 Lecture 23

The main focus for today is to prove the below theorem:

Theorem 71

If $n \in \mathbb{Z}$ is a nonsquare integer, then n is a quadratic nonresidue for infinitely many primes.

Definition 72 (Jacobi symbol)

If $b \in \mathbb{Z}_{>0}$ is an odd integer with prime factorization $b = p_1 \cdots p_n$ and $a \in \mathbb{Z}$, then the symbol $(a/b) := (a/p_1)(a/p_2)\dots(a/p_n)$ where everything on the RHS is a Legendre symbol.

The Jacobi system essentially expands the Legendre symbol to composite denominators.

Lemma 23.0.1

Let r, s be odd integers. Then,

$$(rs-1)/2 \equiv (r-1)/2 + (s-1)/2 \pmod 2$$

and

$$(r^2s^2-1) \equiv (r^2-1)/8 + (s^2-1)/8 \pmod 2.$$

Proof. If r, s are odd, then $(r-1)(s-1) \equiv 0 \pmod 4$. Therefore, $rs - 1 \equiv (r-1) + (s-1) \pmod 4$. Dividing by 2 gives us that $(rs-1)/2 \equiv (r-1)/2 + (s-1)/2 \pmod 2$. □

We observe that $4|r^2-1$. Therefore,

$$\begin{aligned} & (r^2-1)(s^2-1) \equiv 0 \pmod{16} \\ \implies & r^2s^2 - r^2 - s^2 + 1 \equiv 0 \pmod{16} \\ \implies & r^2s^2 - 1 \equiv (r^2-1) + (s^2-1) \pmod{16}. \end{aligned}$$

Dividing by 8 gives us $(r^2s^2-1)/8 \equiv (r^2-1)/8 + (s^2-1)/8 \pmod 2$. □

Corollary 73

If $r_1, \dots, r_n$ are odd integers, then

$$\sum_{i=1}^{n} (r_i - 1)/2 \equiv (r_1 \cdots r_n - 1)/2 \pmod 2$$

and

$$\sum_{i=1}^{n} (r_i^2 - 1)/2 \equiv (r_1^2 \cdots r_n^2 - 1)/8 \pmod 2.$$

Proof. Induct on n, $n = 2$ by the above lemma. Assume the result for n and then for $n+1$ we have

$$\begin{aligned} \sum_{i=1}^{n+1} (r_i - 1)/2 &= \sum_{i=1}^{n} (r_i - 1)/2 + (r_{n+1} - 1)/2 \\ &= (r_1 \cdots r_n - 1)/2 + (r_{n+1} - 1)/2 \\ &\equiv (r_1 \cdots r_{n+1} - 1)/2 \pmod 2. \end{aligned}$$

□

Proposition 74 (i) $(-1/b) = (-1)^{(b-1)/2}$

(ii) $(2/b) = (-1)^{(b^2-1)/8}$

(iii) $(a/b_1b_2) = (a/b_1)(a/b_2)$.

We prove this proposition somehow, then use the proof of that to prove the theorem

24 Lecture 24

Theorem 75 (Quadratic Reciprocity)

If p, q are odd primes then

$$(p/q)(q/p) = (-1)^{((p-1)/2\cdot(q-1)/2))}.$$

Our proof will use the roots of unity.

25 Lecture 25

25.1 Algebraic Numbers

Definition 76

A complex number s is an **algebraic number** if it satisfies a polynomial equation with rational coefficient.

It is an **algebraic integer** if it satisfies a monic polynomial equation with rational coefficients.

These are represented as $\bar{\mathbb{Q}}, \bar{\mathbb{Z}}$, respectively.

If a number is not algebraic, then it is **transcendental**.

26 Lecture 26

26.1 Rings, Fields

Definition 77 (Ring)

A **ring** R is a set R closed under binary operations $+$ and $\cdot$, with the property that

1. $(R, +)$ is an abelian group.
2. Multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. Multiplication distributes over addition: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Definition 78 (Field)

A commutative ring, where every nonzero element has a multiplicative inverse is called a **field**.

Proposition 79

$\overline{\mathbb{Z}}$ forms a ring.

Definition 80

A finite $\mathbb{Z}$-submodule of $\mathbb{C}$ is a subset $\mathbf{V}$ of $\mathbb{C}$ with the property that

1. $v + w \in \mathbf{V}$ if $v, w \in \mathbf{V}$.
2. There exist $v_1, \ldots, v_n \in \mathbf{V} \subset \mathbb{C}$ so that $\mathbf{V} = \{a_1 v_1 + \cdots + a_n v_n \mid a_i \in \mathbb{Z}\}$.

Lemma 26.1.1

If we have a finite $\mathbb{Z}$-submodule $\mathbf{V}$ of $\mathbb{C}$, and $\alpha \in \mathbb{C}$ such that $\alpha\mathbf{V} = \mathbf{V}$, then α is an algebraic integer.

Proof. α on $\mathbf{V}$ is given an $n \times n$ matrix with integer coefficients. □

Proposition 81

If α is an algebraic number, then α is a root of an irreducible unique monic polynomial $g(x) \in \mathbb{Q}[x]$. If $h(x) \in \mathbb{Q}[x]$ has $h(\alpha) = 0$, then $g(n) \mid h(x)$.

Proof. Here, we assume that $g(x)$ is irreducible. If $g(x) \nmid h(x)$, then $(g(x), h(x)) = 1$. Then, it follows that $r(x)g(x)+s(x)h(x) = 1$ for some r, s and any x. However, for $x = \alpha$, we have $g(\alpha) = h(\alpha) = 0$, so this cannot be true. Therefore, $g(x) \mid h(x)$. □

Therefore, the $g(x)$ so described is called the **minimal polynomial** of α.

Definition 82

If $\alpha \in \mathbb{C}$, let $\mathbb{Q}(x)$ denote the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and α.

Then $\mathbb{Q}(x) = \left\{ \frac{g(x)}{h(x)} \mid g(x), h(x) \in \mathbb{Q}[x], h(x) \in 0 \right\}$. $g(x), h(x)$ are polynomials, and $g(x)$ is obtained by substituting α for x.

27 Lecture 27

27.1 Congruence

If $\omega_1, \omega_2, \gamma \in \mathbb{Z}$, we say $\omega_1 \equiv \omega_2 \pmod{\gamma}$ if $(\omega_1 - \omega_2) = \alpha\gamma$, with $\alpha \in \bar{\mathbb{Z}}$.

Lemma 27.1.1

If p is a prime, $\omega_1, \omega_2 \in \mathbb{Z}$, then $(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p \pmod{p}$.

Proof. This is essentially a proof that all of the middle terms are divisible by p. $(\omega_1 + \omega_2)^p$ can be expanded via the binomial theorem, to get that $\left(\frac{p}{n}\right)$ and $p \mid \binom{p}{n}$ if $1 \leq n \leq p$.

A proof of the quadratic character of 2 via Gaussian sums: □

Definition 83

$g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}$ is an example of a quadratic Gauss sum.

Lemma 27.1.2

h

Corollary 84

$$p^{-1} \sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta(x, y) = \begin{cases} 1 & x \not\equiv y \pmod{p} \\ 0 & x \equiv y \pmod{p} \end{cases}.$$

28 Lecture 19

Last time we showed that if m has primitive roots and if $(a, m) = 1$, then $x^n \equiv a \pmod{m}$ has a solution if and only if $a^{\phi(m)/d} \equiv 1 \pmod{m}$, where $d = (\phi(m), n)$.

Remark 85

If $x^n \equiv a \pmod{m}$ has a solution (a, m, n) as above, then it has $(n, \phi(m))$ solutions.

Proof. If g is a primitive root for m, x □

In particular, if $m = p$ is prim,e then $x^n \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/d} \equiv d \pmod{p}$, wherre $d = (p-1, n)$.

If $n = z \neq p$, we have $x^2 \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/z \equiv 1 \pmod{p}}$.

Lemma 28.0.1

Suppose $m \equiv 2^e p_1^{a_1} \cdots p_l^{a_l}$ if a prime factorization of $m \in \mathbb{Z}_{>0}$ and $(a, m) = 1$. Then a is a quadratic residue mod m iff

(a) If $e = 2$, then $a \equiv 1 \pmod{4}$
If $e \geq 3$, then $a \equiv 1 \pmod{8}$.

(b) $a^{(p_i-1)/2} \equiv 1 \pmod{p_i}$ for all i.

Lemma 28.0.2

If p is an odd prime, p not dividing a or n, then if $x^n \equiv a \pmod{p}$ has a solution, then $x^n \equiv a \pmod{p^e}$ is solvable for every $e \geq 1$. All these congruences have the same number of solutions.

Lemma 28.0.3

Let 2^l be the highest power of 2 which divides n. Suppose a is odd and that $x^n \equiv a \pmod{2^{2l+1}}$ is solvable. Then, $x^2 \equiv a \pmod{2^l}$ is solvable for all $e \geq 1$, and all these congruence equations have the same number of solutions.

29 Cubic Equations

Today, we'll look at solutions of $x^2 + y^2 = 1$ in $\mathbb{Z}/p\mathbb{Z}$ for $p \equiv 1 \pmod{3}$.

Recall the definition of Jacobi sumbs gives us $J(\chi, \chi) = \sum_{a+b=1} \chi(a)\chi(b)$ for cubic character χ.

For ω a 3rd root of unity, we see that χ takes values in $\{1, \omega, \omega^2\}$. So this means that $J(\chi, \chi) = a + b\omega$.

Proposition 86

We have that $a \equiv -1 \pmod{3}$ and $b \equiv 0 \pmod{3}$.

Proposition 87

Let $A = 2a - b$ and $B = b/3$. Then, $4p = A^2 + 27B^2$ and $A \equiv 1 \pmod{3}$.

Theorem 88

Suppose $p \equiv 1 \pmod{3}$. Then, there are integers $\overline{A}$ and B such that $4p = A^2 + 27B^2$. If we ask that $A \equiv 1 \pmod{3}$, then A is unieuqly determined.

Moreover, we would have that $N(x^3 + y^3 = 1) = 2p + A$.

Proof. We recall that $N(x^3 + y^3 = 1) = p \cdot 2 + 2 \operatorname{Re} J(\chi, \chi)$.

Therefore, as $J(\chi, \chi) = a + b\omega$, we observe that $\operatorname{Re} J(\chi, \chi) = a - b/2$. So, $2 \operatorname{Re} J(\chi, \chi) = 2a - b = A \equiv 1 \pmod{3}$. □

30 General n

This is 8.4 in the book.