Number Theory

MATH 354, YALE UNIVERSITY, SPRING 2019

These are lecture notes for MATH 354b, "Number Theory," taught by Ross Berkowitz at Yale University during the spring of 2019. These notes are not official, and have not been proofread by the instructor for the course. They live in my lecture notes respository at

https://github.com/jopetty/lecture-notes/tree/master/MATH-354.

If you find any errors, please open a bug report describing the error and label it with the course identifier, or open a pull request so I can correct it.

Contents

1 January 14, 2019

Didn't go to lecture today.

2 January 16, 2019

2.1 Review from last time

Some definitions from last time.

Definition (Divisibility)**.** We say that a divides b if $b = ac$ for some $c \in \mathbf{Z}$. *Divisibility*

Definition (Division Algorithm)**.** Fix a and b. We want to divide a by b. Then there exists some unique q and some $0 \leq r \leq a$ such that $b = aq + r$. *Division Algorithm*

Definition (Prime)**.** A number is prime if its only positive divisors are 1 and itself. *Prime*

These are things we learned in grade school.

Theorem 2.1 (Well-Ordering Principle)**.** *Every nonempty subset of $\mathbf{Z}_{<0}$ has a least element. This is the defining property of $\mathbf{Z}$.*

2.2 Today

Definition (GCD)**.** Let $a, b \in \mathbf{Z}$. The greatest common divisor is the largest common divisor of a and b, so $\gcd(a, b) = \max\{d \mid d \text{ divides } a \text{ and } b\}$. We know this exists because of well-ordering. *GCD*

Definition (GCD)**.** Alternatively, the gcd of a and b is a d such that all other common divisors of a and b divide d as well. Eventually we'll prove that these are equivalent. *GCD*

Definition (GCD)**.** Given a and b in some PID, we say that the GCD is he principal generator d of the ideal (a, b), so $(a, b) = (d)$. Alternatively, the gcd is the smallest positive number in (a, b) if we're working in $\mathbf{Z}$. *GCD*

Notation (GCD)**.** As a nod to the last definition, we often write the GCD of two numbers as (a, b) to emphasize the relation to ideals. *GCD*

Some properties of greatest common divisors:

Lemma 2.2. *Let d be the greatest common divisor of a and b. Then for any $x \in \mathbf{Z}$ we know that $(a, b + ax) = d$ as well. Then the GCD is unchanged under linear combinations.*

Proof. It's clear that d still divides $b + ax$ if it divides a and b, so its clear that $(a, b + ax) \geq (a, b)$. Independently, we know that there can't be a larger divisor

since if d' divides $b+ax$ then d' divides b, and we already know that d is the largest divisor of b which also divides ax. Thus $(a, b+ax) \leq (a, b)$ so $(a, b+ax) = d$. ■

Lemma 2.3. *Let $I = \{ax + by \mid x, y \in \mathbf{Z}\} = (a, b)$. Then $I = \{dx \mid x \in \mathbf{Z}\}$ where d is the greatest common divisor of a and b.*

Proof. We show containment each way. First we note that $I \subseteq d\mathbf{Z}$ since every element of I is divisible by d since if d divides a and b then it divides $ax + by$. Then we show that $d\mathbf{Z} \subseteq I$ (this is sometimes called Bezout's Lemma). By the Well-Ordering property, we know that there exists some $c = \min(I \cap \mathbf{Z}_{>0})$. We know that $c \geq d$ since it must be the case that d divides c. On the other hand, if we can show that c is a common divisor of a and b then we know that $c \leq d$ as well. We know that $a = cq + r$ for $0 \leq r \leq c$. Then we know that $c \in I$ implies that $c = ax + by$ so $r = a - cq = a(1 - xq) + b(-yq)$ so $r \in I$. Since c is the minimum positive element we know that $c = 0$ and so $a = cq$ so it divides a. Repeat for b. Then $c \leq d$ and $c \geq d$ so $c = d$. This also gives us the definition of the GCD which is the divisor of a and b which is divisible by all other common divisors. ■

This part could be proved with the Extended Euclidean Algorithm.

Uniqueness of prime factorization

Lemma 2.4. *Let a and b be relatively prime. If a divides bc then a divides c.*

Proof. Note that $(a, b) = 1$, so there exist some $x, y \in \mathbf{Z}$ such that $1 = ax + by$. Multiplying through by c, we get that

$$c = cax + cby.$$

Since a divides cb it divides cby and it trivially divides cax so a divides c. ■

Corollary 2.5. *If p is prime and p divides ab then p divides a or p divides b.*

Corollary 2.6. *If p divides $\prod a_i$ then for some i we know that p divides a_i (this is the above corollary with induction).*

Theorem 2.7. *All integers have a unique prime factorization. For every $n \in \mathbf{Z}_{\geq 2}$ there exists a unique set of primes $p_1, \cdots, p_k$ and positive integers $a_1, \cdots, a_k$ such that $n = \prod_{i=1}^{k} p_i^{a_i}$.*

Proof. Assume that we have two (more than one) such lists of primes and their powers. Denote them $P = p_1, \cdots, p_k$ (possible with repeats) and $Q = q_1, \cdots, q_\ell$. Assyme by way of contradiciton that the lists are disjoint (otherwise we cancel the like terms). We know that p_1 divides $\prod_{i=1}^{\ell} q_i$, so p_1 must divide q_i for some i. This can happen if and only if $p_1 = q_i$. This contradicts the disjointness of our list and presents a contradiciton. ■

2.3 Before next class

1. Read §1.1 – §1.3 in *Ireland and Rosen*;
2. Read §3, §4.1, and §4.2 in *Rosen*;
3. Think about which textbook is preferred.

3 Lecture 3

Didn't take notes today.

4 Wednesday, January 23

Recall the uniqueness of prime factorization, where for all $n \in \mathbf{N}$ we have a unique list of primes $p_1, \dots, p_k$ and $a_i, \dots, a_k \in \mathbf{Z}_{>0}$ such that $n = \prod_{i=1}^{k} p_i^{a_i}$.

4.1 Infinitude of Primes

Problem 4.1. How many primes are there?

Theorem 4.1. *There are infinitely many primes.*

Euclid's Proof. Assume by way of contradiction we have a finite list of primes $p_1, \dots, p_k$ of all primes. Let $M = \prod p_i$, and consider $M + 1$. By the existence of prime factorization, we know that $M + 1 = \prod_{i=1}^{k} p_i^{a_i}$. Without a loss of generality assume that $a_1 \neq 0$. Then p_1 divide $M + 1$ and since p_1 divides M it must be the case that p_1 divides 1 as well which presents a contradiction. ■

Fact: Let $p_1, p_2, p_3, \dots$ be a list of primes in order. By the uniqueness of prime factorization, there is an injective correspondence between vectors $(a_1, a_2, \dots) \in (\mathbf{Z}_{\geq 0})^{\infty}$ with finitely many nonzero entries and $\mathbf{N}$. The correspondence is $n = \prod p_i^{a_i}$ with a lot of a_i being zero.

NOTE: THE BELOW IS BY CONTRADCTION and (*) ONLY HOLDS FOR $k = \infty$. If we assume that the list of primes is finite, then we would have an injective correspondence between $(a_1, \dots, a_k) \in (\mathbf{Z}_{\geq 0})^k$ and $\mathbf{N}$. Therefore

$$\prod_{i=1}^{k} \left(\sum_{j=0}^{\infty} \frac{1}{p_i} \right) = \sum_{n=1}^{\infty} \frac{1}{n}. \tag{*}$$

Then by uniqueness of prime factorization for each $n \in \mathbf{N}$ we know that $1/n$ appears exactly once when you expand this product. This is Euler's product for the ζ function?

Euler's Proof. Assume by way of contradiction that there are finitely many primes. Then

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{i=1}^{k} \left(1 + \frac{1}{p_1} + \cdots \right) = \prod_{i=1}^{k} \left(\frac{1}{1 - 1/p_i} \right) < \infty.$$

Yet we know that $\sum 1/n$ diverges, which presents a contradiction. ■

Lemma 4.2. *For any $n \in \mathbf{Z}$ there exists a unique $a, b \in \mathbf{Z}$ such that a is square free (meaning that no square number divides it) and $n = ab^2$.*

Erdős' Proof. Assume by way of contradiction that there are finitely many primes. Then any square-free number $n = \prod p_i^{a_i}$ where $a_i \in \{0, 1\}$. Thus there are only 2^k

square-free numbers. Now let's look at all numbers at most N for some N. By the above lemma, they can be specified by (a, b) where a is square-free and b^2 is square. There are 2^k square-free numbers and at most $\sqrt{N}$ square numbers, so $N \leq 2^k\sqrt{N}$ for all N, so $2^k \geq \sqrt{N}$ for all N, which is very very false if $N > 2^{2k}$. ■

4.2 Congruence Equations & Modular Arithmetic

Congruence

Definition (Congruence)**.** We say that $a \equiv b \pmod{m}$ if and only if m divides $b - a$. Alternatively, we say that $a \equiv b \pmod{m}$ if and only if there exists some k such that $a = b + mk$.

Theorem 4.3 (Some quick remarks)**.**

1. *Congruency is an equivalence relation on the integers (transitive, symmetric, and reflexive);*
2. *For some fixed m, we define the congruence class $\bar{a}$ to be the set $\bar{a} = \{n \in \mathbf{Z} \mid n \equiv a \pmod{m}\}$;*
3. *Arithmetic on these congruence classes holds; If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a+c \equiv b+d \pmod{m}$ and $ac \equiv bd \pmod{m}$. Thus $\bar{a}+\bar{b} = \overline{a+b}$ and $\bar{a}\bar{b} = \overline{ab}$. This forms the commutative ring $\mathbf{Z}/m\mathbf{Z}$.*

Problem 4.2. Let a, b, m be fixed. When is the congruence $ax \equiv b \pmod{m}$ solvable?

Obs. 1. If $(a, m) = 1$ then we can use Bezout's theorem. This tells us that tehre exist some X, Y such that $1 = aX + mY$. Then we multiply through by b to get that $b = a(Xb) + m(Yb)$. Then $aXb \equiv b \pmod{m}$.

Lemma 4.4. *The congruence $ax \equiv b \pmod{m}$ has solutions if and only if the* GCD *of a and m divides b.*

Proof. Let d be the GCD of a and m. By Bezout, there exists some $X_0, Y_0 \in \mathbf{Z}$ such that $d = aX_0 + bY_0$. Since d divides b there exists some k such that $b = dk$. Then $b = aX_0k + mY_0k$ so $b \equiv aX \pmod{m}$ for $X = X_0k$. In the other direction, just write it out. If there is a solution then $b \equiv aX \pmod{m}$ so $b = aX + mY$. Since the GCD divides the right hand side it must divide the left as well, so d divides b. ■

Problem 4.3. Can there be lots of different solutions? What do solutions look like?

5 Monday, January 28

5.1 Solving $ax \equiv b \pmod{m}$

Recall from last lecture that $ax \equiv b \pmod{m}$ is solvable if and only if the GCD divides m. If we let $m' = m/d$ then the solutions are unique modulo m'.

Proof. Let x_1, x_2 be solutions to $ax_1 \equiv b \pmod{m}$ and $ax_2 \equiv b \pmod{m}$. Consider then that $a(x_1 - x_2) \equiv 0 \pmod{m}$. Let $a' = a/d$. Then $da'(x_1 - x_2) = dm'k$. We know that m' divides $a'(x_1 - x_2)$, and since $(m', a') = 1$ we know that m' divides $x_1 - x_2$. ■

Corollary 5.1. *If $(a, m) = 1$ then there is a unique solution to $ax \equiv b \pmod{m}$.*

Corollary 5.2. *If $a \not\equiv 0 \pmod{p}$ for prime p then there is a unique solution to $ax \equiv b \pmod{p}$ in $\mathbf{Z}/p\mathbf{Z}$.*

Chinese Remainder Theorem

Theorem 5.3 (Chinese Remainder Theorem)**.** *If we have $m_1, \ldots, m_r$ all relatively prime and the system of equations*

$$x \equiv a_1 \pmod{m_1}, \ldots, a \equiv a_r \pmod{m_r},$$

then there is a unique solution modulo $M = m_1 \cdots m_r$. Alternatively, the rings

$$\mathbf{Z}/M\mathbf{Z} \equiv \bigoplus_{i=1}^{r} \mathbf{Z}/m_i\mathbf{Z}$$

are isomorphic.

Lemma 5.4. *If $a_1, \ldots, a_r$ are pairwise relatively prime to m then the product $a_1 \cdots a_r$ is also relatively prime to m as well.*

Lemma 5.5. *If $a_1, \ldots, a_r$ all divide m and are all pairwise relatively prime to m then the product $a_1 \cdots a_r$ divides m.*

Proof of CRT. Let $\hat{M}_i = M/m_i = \prod_{j \neq i} m_i$. We find a helper y_i such that $y_i \equiv 0 \pmod{\hat{M}_i}$ and $y_i \equiv 1 \pmod{m_i}$. Then we'll have that $x = \sum a_i y_i$. Note that $(\hat{M}_i, m_i) = 1$ so we know that $1 = x_i\hat{M}_i + y_i m_i$ has a solution. Let $y_i = x_i\hat{M}_i$. THis shows existence. To show uniqueness, just apply Lemma 5.2 above. ■

5.2 Algorithmic Speed for the Chinese Remainder Theorem

The Euclidean Algorithm runs in logarithmic time in the inputs a, b. The worst case is when we plug in two consecutive Fibonacci numbers since they are recursively defined in almost the exact opposite way that Euclid's algorithm reduces numbers.

6 Wednesday, January 30

6.1 Pollard-ρ Factorization

We want to factor n. If we can find $0 < a, b < n$ such that $a \equiv b \pmod{p}$ then $(b-a, n) = p$ is a nontrivial factor of n. Our first idea was to try numbers at random, and after about $\sqrt{p}$ samplings we'll find two a, b which are congruent mod p. But since there were $\binom{\sqrt{p}}{2}$ pairs so it takes about $p \log p$ steps.

New idea: Start at $x_0 = 2$. For $i \geq 1$, let $x_{i+1} = x_i^2 + 1 \pmod{n}$. This will replace our random numbers, and the hope is that this sequence $x_1, x_2, \ldots$ is "random enough" for our uses. Now if $x_j \equiv x_i \pmod{p}$ for any p dividing n then $x_{j+1} = x_j^2 + 1 \pmod{n} \equiv x_j^2 + 1 \pmod{p} \equiv x_i^2 + 1 \pmod{p} \equiv x_{i+1} \pmod{p}$. This forms a nice cycle modulo p.

6.2 Floyd's Cycle Finding

Given a sequence $a_1, a_2, \ldots$ which is eventually periodic (where repeats indicate multiples of the period), how do we find the period of the sequence? That is, we have no guarantee that a_1 will reappear, but we know that the sequence will eventually have a repeating part. Ideas:

1. Pick pairs at random. Really inefficient.
2. Fix a_1 and check all the others in the list until you find a match. But we have no idea when the cycle starts.

Instead we use a "tortoise adn the hare method," where we have two pointers in our sequence. The slow pointer t moves through the list while the fast pointer h moves twice as fast as the tortoise. Eventually both of the following will happen:

1. $t_i = x_i$ in the sequnce, and
2. the length of the cycle ℓ divides i

and then $t_i = h_i$ and we have a multiple of the cycle length.

6.3 Algorithm

Let $x_0 = 2$ and let $x_{i+1} = x_i^2 + 1 \pmod{n}$.

Step 1. Compute $(x_{2i} - x_i, n)$. If this equals 1, continue. Otherwise it is a nontrivial factor of n.

If the x_i are sufficiently random, then with high probability there are two $j, k \leq O(\sqrt{p})$ such that $x_j \equiv x_k \pmod{p}$ where p is any divisor of n. After $O(\sqrt{p})$ steps we will have

- $k - j$ divides i;
- $i \geq \min(j, k)$;

These imply that x_i is in the cycle and that $x_{2i} \equiv x_i \pmod{p}$. Then $x_i \equiv x_{i+(k-j)} \pmod{p}$. Then $(x_{2i} - x_i, n)$ is at least p, a nontrivial factor.

Pollard-ρ runs in about $O(n^{1/4} \log n)$, which is $O(n^{1/4})$ computations of the GCD, and it runs especially quickly in the case that n has small prime factors since those determine the cycle length.

6.4 Some cool things

Theorem 6.1. *If p is prime then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. Every number can be paired with its mutliplicative inverse in $\mathbf{Z}/p\mathbf{Z}$. Then $(p-1)! = \prod a = \prod_{(a,a^{-1})}(a \cdot a^{-1}) \cdot -1 = -1$ (this double counts when $a = a^{-1}$, so when $a = \pm 1$). ■

Theorem 6.2 (Fermat's Little Theorem)**.** *For prime p, $x^p \equiv x \pmod{p}$ for any $x \in \mathbf{Z}$.*

Proof. Recall $\varphi(n)$ is the number if numbers less than n which are relatively prime to n, and let $\mathbf{Z}/m\mathbf{Z}^\times$ is the set of units in $\mathbf{Z}/m\mathbf{Z}$, which is the set of numbers relatively prime to m equipped with multiplication modulo m. ■

7 Monday, February 4

Recall that if p is prime then $a^{p-1} \equiv_n 1$, which gives us a suggested primality test: If we want to know if p is prime, pick some $1 \leq a \leq p$ and check $a^{p-1} \pmod{p}$. This doesn't always $4^{14} \equiv_{15} 1$. The question now becomes, is this a rarity?

Pseudoprime

Definition (Pseudoprime)**.** A nonprime integer n is a pseudoprime to the base b if $b^{n-1} \equiv_n 1$.

Theorem 7.1. *Fix a base $b = 2$ with at least one odd pseudoprime n. There are infinitely many pseudoprimes to the base $b = 2$.*

Proof. Consider $m = b^n - 1$. We know that $b^n - 1 = (b-1)(b^{n-1} + b^{n-1} + \cdots + 1)$. Since n is a pseudoprime, we know we may write it as $n = ac$ where $a, c \neq 1$, and we know that $b^n \equiv_n b$. Then n divides $b^n - b$. We also know that m is not prime since $b^a - 1$ divides $b^n - 1$. For now, let $b = 2$. Now consider $b^{m-1} = b^{b^n - 2} = 2^{2^n - 2}$. We know that both n and $2^n - 1$ divide 2^{2^n-2}. Then m divides $2^{m-1} - 1$ so $2^{m-1} \equiv_m 1$. ■

Corollary 7.2. *There are infinitely many pseudoprimes to the base 2.*

Carmichael Number

Definition (Carmichael Number)**.** An integer n is a Carmichael number if for any base b which is relatively prime to n we have $b^{n-1} \equiv_n 1$. This means that the Fermat test for primality fails *spectacularly.*

Theorem 7.3. *There are infinitely many Carmichael numbers.*

We will return to this theorem in a few weeks and extend it to the Miller Primality Test.

7.1 Rosen 7.1

Recall Euler's Totient Function $\varphi(n)$, which is weakly multiplicative in that $\varphi(nm) = \varphi(n)\varphi(m)$ when $(n, m) = 1$. We also know that $\varphi(p^\ell) = p^\ell - p^{\ell-1}$ for prime p.

Here is a fact: $\sum_{d|n} \varphi(d) = n$.

Proof. Look at the following sequence

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n},$$

when written in reduced form. For any fixed denominator d, it shows up $\varphi(d)$ times in this sequence. We wrote n numbers, so $n = \sum_d \varphi(d)$. ■

7.2 Multiplicative Structure of $\mathbf{Z}/n\mathbf{Z}$

Recall that $(\mathbf{Z}/n\mathbf{Z})^\times$ is the multiplicative group of units in $\mathbf{Z}/n\mathbf{Z}$. Our goal is to understand "When is this group cyclic?" This amounts to asking "Is there an element of order $\varphi(n)$?" Such an element, if it exists, is called a *primitive root* modulo n.

> **Definition** (Order)**.** The order of $r \in G$ is the smallest $a > 0$ such that $r^a = e \in G$. *Order*

Theorem 7.4. $(\mathbf{Z}/p\mathbf{Z})^\times$ *is cyclic for prime* p*.*

Lemma 7.5. *It is always true that the order of* r *modulo* p *is a divisor of* $p-1$*.*

Proof. Lagrange's Theorem. ■

8 No Notes

9 No Notes

10 Wednesday, 23 February

Recall the question of when is $(a/p) = \pm 1$ when $a \in \mathbf{Z}$, $(a,p) = 1$, and p is prime. We defined $|x| = \min\{x, p-x\}$ for $0 \le x \le p-1$. Recall Gauss' Lemma, which states

Lemma 10.1 (Gauss)**.** *Let s be the number of ℓ such that $1 \le \ell \le (p-1)/2$ such that $|a\ell| = -a\ell$. Then $(a/p) = (-1)^s$.*

> **Example 10.1.** Let $p = 17$ and let $a = 2$. Then $\{a\ell\}$ is $\{2,4,6,8,10,12,14,16\}$. We see that $(p+1)/2 = 9$. Then $s = 4$ and so $(2/p) = 1$.

Theorem 10.2. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv_8 \pm 1, \\ -1 & p \equiv_8 \pm 3. \end{cases}$$

Proof. We just need to look at how many even numbers are between 1 and $(p-1)/2$ verses $(p+1)/2$ and p.

Case 1: $p = 1 + 8k$. Then $(p-1)/2 = 4k$, so $s = 2k$ and $(2/p) = (-1)^{2k} = 1$.

Case 3: $p = 3+8k$. Then $(p-1)/2 = 4k+1$, so there are $2k$ even numbers ebtween 1 and $(p-1)/2$ and $2k+1$ even numbers between $(p+1)/2$ and p, so $(2/p) = -1$. ∎

What about (p/q) when p and q are odd primes.

Theorem 10.3 (Quadratic Reciprocity)**.** *If $p \equiv_4 1$ or $q \equiv_4 1$ then $(p/q) = (q/p)$. Otherwise, if $p \equiv_4 q \equiv_4 3$ then $(p/q) = -(q/p)$. Equivalently,*

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

Proof. Consider $f(z) = 2i\sin(2\pi z)$, which has some nice properties. It's odd, so $-f(z) = f(-z)$. It's also 1-periodic, so $f(z) = f(z+1)$. Note that $i\sin(z) = \sinh(iz)$, so

$$f(z) = e^{2\pi i z} - e^{-2\pi i z}.$$

Define $\zeta = \zeta_p$ to be the p^{th} root of unity $2^{2\pi i/p}$. Note that $\zeta^m \cdot \zeta^n = \zeta^{m+n \mod p}$ and $(\zeta^m)^\ell = \zeta^{m\ell \mod p}$

We also have the following Proposition and Lemma, listed after the proof.

Now let p, q be odd primes. Then

$$\left(\frac{q}{p}\right) = \prod_{\ell=1}^{(p-1)/2} \frac{f(q\ell/p)}{f(\ell/p)} = \prod_{\ell=1}^{(p-1)/2} \prod_{k}^{(q-1)/2} f\left(\frac{\ell}{p} + \frac{k}{q}\right) f\left(\frac{\ell}{p} - \frac{k}{q}\right).$$

Notice how this expression is almost symmetric in p and q, with only one difference in the final term. In fact, switching them out only requires $(-1)^{(p-1)(q-1)/2}$. ∎

Proposition 10.4. *Consider that*

$$\prod_{\ell=1}^{(p-1)/2} f\left(\frac{a\ell}{p}\right) = \left(\frac{a}{p}\right) \cdot \prod_{\ell=1}^{(p-1)/2} f\left(\frac{\ell}{p}\right).$$

The justification comes from the periodicity of f.

Proof. Consider that if $1/2 < a\ell/p < 1$ then

$$f\left(\frac{a\ell}{p}\right) = -f\left(\frac{|a\ell|}{p}\right).$$

Then

$$\prod_{\ell=1}^{(p-1)/2} f\left(\frac{a\ell}{p}\right) = (-1)^s \prod_{\ell=1}^{(p-1)/2} f\left(\frac{|a\ell|}{p}\right) = \left(\frac{a}{p}\right) \prod_{\ell=1}^{(p-1)/2} f\left(\frac{|a\ell|}{p}\right).$$

Then recall that the sequence $\{|a|, |2a|, \dots, |(p-1)a/2|\}$ is just $\{1, 2, \dots, (p-1)/2\}$, which gets us that

$$\left(\frac{a}{p}\right) \prod_{\ell=1}^{(p-1)/2} f\left(\frac{|a\ell|}{p}\right) = \left(\frac{a}{p}\right) \prod_{\ell=1}^{(p-1)/2} f\left(\frac{\ell}{p}\right).$$ ∎

Lemma 10.5. *If n is odd then*

$$x^n - y^n = \prod_{k=0}^{n} \left(x\zeta^k - y\zeta^{-k}\right),$$

where $\zeta = \zeta_n$.

Proof. It suffices to look at $(x/y)^n - 1 = z^n - 1$, which factors as

$$z^n - 1 = \prod_{k=0}^{n-1} \left(z - \zeta^k\right) = \prod_{k=0}^{n-1} \left(z - \zeta^{-2k}\right).$$

Then

$$x^n - y^n = \prod \left(x - y\zeta^{-2k}\right) = \left[\prod \left(x\zeta^k - y\zeta^{-k}\right)\right] \zeta^{-(n-1)/2},$$

where $\zeta^{-(n-1)/2} = 1$ since n is odd. ∎

Lemma 10.6. *The value*

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right)$$

if n is odd.

Proof. Notice that $f(nz) = e^{2\pi i z n} - e^{-2\pi i z n}$. Now just apply the previous lemma. ∎

10.1 Applications of QR

Example 10.2 (We can use it to compute Legendre Symbols!)**.** Compute

$$\left(\frac{713}{1009}\right).$$

We factor as

$$\left(\frac{23\cdot 31}{1009}\right)=\left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)=\left(\frac{1009}{23}\right)\left(\frac{1009}{31}\right)=\left(\frac{20}{23}\right)\left(\frac{17}{31}\right).$$

Definition (Jacobi Symbol)**.** Let (q/n) be the Jacobi symbol, where n is a product of primes, then it is multiplicative. *Jacobi Symbol*

$$\left(\frac{q}{n}\right)=\begin{cases}0 & (a,n)\neq 1,\\ \prod\left(\frac{a}{p_i}\right)^{1/i} & (a,n)=1.\end{cases}$$

Theorem 10.7 (Jacobi Reciprocity)**.** *Some facts:*

- $(-1/n)=(-1)^{(n-1)/2}$
- $(2/n)=(-1)^{(n^2-1)/8}$
- *If* m,n *odd then* $(m/n)(n/m)=(-1)^{(m-1)(n-1)/4}$

Next Class

- Use Jacobi to talk about when a is a quadratic residue for almost all primes
- RSA/Diffie-Hellman, Zero Knowledge Proofs

11 Monday, 18 February

Recall the definition of the Jacobi Symbol. This is like the multiplicative extension of the Legendre Symbol, although we loose the nice property that $(a/n) = 1$ if and only if a is a quadratic residue modulo n. We do that the following properties:

$$\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right) \qquad \text{and} \qquad \left(\frac{a}{n}\right)\left(\frac{a}{\ell}\right) = \left(\frac{a}{n\ell}\right).$$

Also recall the theorem of Jacobi Reciprocity, restated here:

Theorem 11.1 (Jacobi Reciprocity)**.** *Some facts:*

- $(-1/n) = (-1)^{(n-1)/2}$
- $(2/n) = (-1)^{(n^2-1)/8}$
- *If m, n odd then* $(m/n)(n/m) = (-1)^{(m-1)(n-1)/4}$

Theorem 11.2. *If a is a non-square, there are infinitely many primes such that $(a/p) = -1$, that is where a is not a residue modulo p.*

Proof. Assume that $a = 2^e \cdot \prod q_i$, where q_i are distinct primes and $e \in \{0, 1\}$. We assume here that a is square free, since we can always reduce the exponents modulo 2 to get rid of this square part. Fix any set of primes $\ell_1, \ldots, \ell_k$ distinct from $2, q_i$. We want to show that there is a prime p not in this list such that $(a/p) = -1$. We do this by building such a number. By CRT we know there is a x such that $x \equiv_8 1 \equiv_{\ell_i} 1 \equiv_{q_{i<m}} 1 \equiv_{q_m} s$, where $(s/q_m) = -1$. Consider that

$$\left(\frac{a}{x}\right) = \left(\frac{2^e}{x}\right)\prod\left(\frac{q_i}{x}\right) = 1 \cdot \prod\left(\frac{x}{q_i}\right) \cdot (-1)^{(x-1)/2\cdot(q-1)/2} = \prod\left(\frac{x}{q_i}\right).$$

Now, since $x \equiv_{q_{i<m}} 1$, we get that

$$\prod\left(\frac{x}{q_i}\right) = 1^{m-1}\left(\frac{s}{q_m}\right) = -1.$$

Then we use the multiplicative nature of the Jacobi symbol to say that

$$\left(\frac{a}{x}\right) = -1 = \prod\left(\frac{a}{p_i}\right) \qquad \text{where } x = \prod p_i^{v_i},$$

and we know that $p_i \neq q_i$ since otherwise its congruence modulo q_i would be zero. Since we already know this equals -1, there must be *some* (at least one) p_i such that $(a/p_i) = -1$. This is really similar to Euclid's proof of the infinitude of primes. ■

Note: The above assumes that $a \neq 2$ since we implicitly assumed there was at least one odd prime factor. If $a = 2$, then it is a nonresidue if and only if $p \equiv_8 3, 5$. There are infinitely many primes $p \equiv_8 3$.

11.1 RSA Cryptography

RSA is a public-key cryptography system. Historically, crypto systems has the same encoding and decoding key. An example is something like a cryptogram, like `XYQ ABCX`, where each letter is a swap for another letter in the alphabet, so `XYQ ABCX` $\to$ `THE BOAT`. If you know the bijection $f\colon A \to A$ then you can both encode and decode the message.

> Fun fact, `BEBOPBOP` is a valid cryptogram for exactly one English word.

Another example is Enigma (yay Alan Turing) from WWII, where the ability to read or send the messages was dependent on a (very high) number of possible dial-combinations, which made it easy to use but computationally difficult to break.

Public Key cryptography sets up a system where anyone can encrypt a message for Alice, but only she may decrypt such a message. This is accomplished by having two different keys. In private, Alice will pick two primes p, q and publicly announces their product $n = pq$. Privately, she can compute $\varphi(n) = (p-1)(q-1)$. She the picks an encryption exponent e and announces this too, and then privately computes $d = e^{-1} \bmod \varphi(n)$. Let's say that Bob wants to send a message to Alice. Suppose this message is some number P between 2 and n (1 fails for obvious reasons). Bob takes P and encrypts is via $C = P^e$ and sends C to Alice. When she receives it, she takes $C^d = P^{e^d} \equiv P^{e \cdot e^{-1}} \bmod \varphi(n) = P$. If Eve is looking in on this transmission, she can see $C = P^e$ and she even knows what e is! However, given a composite number n, it is computationally easy to compute $P^e \bmod n$, but it is nearly intractable to find P given P^e. This means that Alice can't really decrypt the message by brute force. Nor can she compute $\varphi(n)$, since it is also very hard to compute $\varphi(n)$ from n; we believe it to be as hard as factoring n, which is not easy to do[1].

[1] *We think this is the case.*

11.2 Diffie-Hellman Key Exchange

Suppose that Alice has a secret she needs to share with Bob. They don't care what the secret is, but they both need to know it (like an Enigma Key!). It would be bad for Alice to announce it publicly, since anyone could hear it and it's not a secret anymore. One better method is for Alice to take the secret and lock it in a box and send it to Bob. Bob can't open it, but neither can anyone else. However, Bob *can* add his own lock to the box, and send it back to Alice. She then unlocks her lock, and sends the box back to Bob, who can not unlock the last remaining lock and read the secret message without anyone else having read it. This is (more or less) how Diffie-Hellman Key Exchange works.

Alice and Bob agree publicly on a public prime p, and some primitive root-ish[2] r. Now they will each privately choose keys k_A and k_B, which they don't reveal to anyone. Alice then transmits $c_A = r^{k_A} \bmod p$ and Bob transmits $c_B = r^{k_B} \bmod p$. Alice takes $c_B^{k_A} = r^{k_A k_B} \bmod p$ and Bob takes $c_A^{k_B} = r^{k_A k_B} \bmod p$. This is their shared secret. Note however that the secret they end up with $r^{k_A k_B} \bmod p$ is different than what they started with it, but they both end up with a shared secret.

[2] *This might be hard to find, so we can find something with a large enough order and just go with that.*

11.3 Zero-Knowledge Proofs

Suppose that Paula knows something (this is good) and she wants to prove that she knows it, but doesn't want to reveal the knowledge. A *Zero-Knowledge Proof* is a protocol whereby she may interact with Vince, the verifier, that she knows this secret.

Example 11.1. Imagine that Vince is color-blind, and cannot tell red from green. Paula has a red sock and a greens sock. When Vince sees these, he can't tell which is which, but Paula wants to prove to Vince that she can distinguish between them. To do this, Paula hands both socks to Vince. In each round,

- Vince will produce a sock (he doesn't know which one), shows it to Paula, and puts it behind his back, and then produces a second sock (either S_1 or S_2) and then asks Paula whether or not it is the same sock.
- Paula answers him each time. If she couldn't tell the difference, she would have to guess which sock it was, and so in total she fails with probability $1 - 0.5^n$ after n rounds. If, however, she *does* see the difference then Vince is confident that she does so with the same probability.

Thus Vince can be as sure as he wants to be that Paula can see the colors without every actually learning which sock is which.

Example 11.2. Paula wants to prove her identity to the world. She picks primes p, q, u in private, and announces to the world "I am Paula! $n = pq$ and $v = u^2$." Then Paula is anyone who knows $\sqrt{v} = u$ without showing what u is. To do so, she will

1. Pick an r at random and sends $x = r^2 \bmod n$ to Vince.

2. Vince receives x and flips a coin. If it is heads, Vince asks, "Send me r." If it is tails, Vince asks, "Send me $r^{-1} \cdot u \bmod n$".

Paula answers with A. Vince verifies that Paula is telling the truth. In the 'heads' regime, Vince checks if $A^2 = x \bmod n$. In the 'tails' regime, he checks if $A^2 x = v \bmod n$.

12 Monday, 25 February 2019

13 Monday, 4 March 2019

It's been a while.

Let p be prime. Recall the following definitions:

- $\Pi(x) = \sum_{p \le x} 1$;
- $\vartheta(x) = \sum_{p \le x} \log p$;
- $\psi(x) = \sum_{p^n \le x} \log p = \sum_{n \le x} \Lambda(x)$.

We had two important results from these definitions.

Theorem 13.1. $|\vartheta(x) - \psi(x)| \le O(\sqrt{x} \log^2 x)$.

Theorem 13.2. $\Pi(x) = \vartheta(x)/\log x - \int_1^x \vartheta(x)/t \log^2 x \, \mathrm{d}t$.

Theorem 13.3. *The following are equivalent:*

- $\psi(x) \sim x$,
- $\vartheta(x) \sim x$,
- $\Pi(x) \sim x/\log x$.

Lemma 13.4. $M_{\log x} = \sum_{n \le x} \log n = x \log x - x + O(\log x)$.

Proof. Consider

$$\sum_{n \le x} \log n \cdot 1.$$

We apply Abel summation using $f(n) = 1$ and $\phi(x) = \log x$ to get that

$$\sum_{n \le x} \log n \cdot 1 = \lfloor x \rfloor \log x - \int_1^x \frac{\lfloor t \rfloor}{t} \, \mathrm{d}t \,,$$

noting that $M_1 = \lfloor x \rfloor$. Notice that

$$\int_1^x \frac{\lfloor t \rfloor}{t} \, \mathrm{d}t = \int_1^x 1 - \frac{t - \lfloor t \rfloor}{t} \, \mathrm{d}t = x - 1 - O\left(\int_1^x \frac{1}{t} \, \mathrm{d}t \right) = x + O(\log x).$$

This acheives the result we wanted. ∎

Theorem 13.5 (Chebyshev)**.** *The inequality*

$$x \log 2 + O(\log x) \le \psi(x) \le x \log 4 + O(\log^2 x)$$

holds.

Proof. Recall that $M_{\log(x)} = \sum_{n \le x} \log n$, and that

$$\log n = \sum_{d \mid n} \Lambda(d).$$

Then

$$M_{\log(x)} = \sum_{n \le x} \sum_{d \mid n} \Lambda(d) = \sum_{dq \le x} \Lambda(d) = \sum_{q \le x} \sum_{d \le x/q} \Lambda(d) = \sum_{q \le x} \psi\left(\frac{x}{q}\right).$$

Define the quantity

$$D(x) = M_{\log}(x) - 2M_{\log}\left(\frac{x}{2}\right) = \log \binom{x}{x/2}.$$

On one had, we can show that

$$D(x) = x \log(2) + O(\log x),$$

and on the other had we know that

$$D(x) = \sum \psi(x/q) - 2 \sum \psi(x/2q) = \psi(x) - \psi(x/2) + \psi(x/3) + \cdots.$$

Note that $\psi(x)$ is "sorta monotone increasing" ■

14 Monday, 25 March 2019

Recall from last lecture (I don't) that we have a theorem:

Theorem. *There are infinitely many primes p satisfying $p \equiv 3 \pmod 4$.*

Lemma. *Let q be prime. There are infinitely many primes $p \equiv 1 \pmod q$.*

Proof. Look at $\Phi_q(x) = \frac{x^q-1}{x-1} = x^{q-1} + \cdots + 1$. We know that if $p \mid \Phi_q(x)$ then $p \equiv 1 \pmod q$. Note that $p \mid x^q - 1$ or $x \equiv 1 \pmod p$. In the former case, we know that the order of x is q, so $q \mid p-1$, which implies that $p \equiv 1 \pmod q$. In the latter case, we would get that $p \mid q$ which is really problematic since p and q are distinct primes.

To prove that there are infinitely many such primes, suppose we have some finite list of primes $p_1, \dots, p_\ell$. Notice that $\Phi_q(x) \equiv 1 \pmod x$ for all x, so let x be the product of these finite primes. Then any prime which divides $\prod p_i$ must itself be congruent to 1 modulo q, and since these prime factors must exist we know that there exist infinitely many primes which are congruent to 1 modulo any prime q. ■

Outline of Dirichlet's Proof

Theorem 14.1. *For any q and any $(a,q) = 1$ there are infinitely many primes of the form $p = a + kq$.*

First, some definitions:

Character

Definition (Character)**.** A character is a homomorphism from an Abelian group G to the complex numbers $\mathbf{C}$.

Example 14.1 (Example of a character)**.** Let $G \simeq (\mathbf{Z}/m\mathbf{Z}, +)$. There are m characters of the form

$$\psi_a(x) = \zeta^{ax},$$

where ζ is the m^{th} root of unity. One may trivially check that this is, in fact, a homomorphism.

A list of facts:

1. The characters of G themselves form an Abelian group $\widehat{G}$, and there are exactly $|G|$ of them.
2. Orthogonality relations.

- $$\sum_{a \in G} \psi(g) = \begin{cases} |G| & \text{if } \psi \equiv 1, \\ 0 & \text{otherwise.} \end{cases}$$
- $$\sum_{\psi \in \widehat{G}} \psi(g) = \begin{cases} |G| & \text{if } g = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Let χ be some character of the group $(\mathbf{Z}/q\mathbf{Z})^\times$.

Dirichlet Character

Definition (Dirichlet Character)**.** The Dirichlet character is a map $\chi \colon \mathbf{N} \to \mathbf{C}$ which extends a regular character by saying that

$$\chi(m) = \chi(\bar{m}) \quad \text{if } m \equiv \bar{m} \pmod{q},$$

and that $\chi(m) = 0$ if $(m, q) \neq 1$.

Example 14.2. Let $q = 5$.

- The trivial character:

$$\chi_o = 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, \ldots$$

- The Legendre symbol

$$\left(\frac{m}{5}\right) = \begin{cases} -1 & m \text{ non residue}, \\ 1 & m \text{ residue}, \\ 0 & m \equiv 0 \pmod{5}. \end{cases}$$

The character is a completely multiplicative function.

L-function

Definition (L-function)**.** Given a Dirichlet character χ, we define the Dirichlet L-function $L(s, \chi) \colon \text{“}\mathbf{C}\text{”} \to \mathbf{C}$ by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

which is just the Dirichlet series of χ.

Example 14.3. Let $\chi = \chi_0$ and let q be prime. Then $L(s, \chi_0) = \sum 1/n^s$ where $n \not\equiv 0 \pmod{q}$.

> Remark — Why care about these characters? Well, they are really good at picking out numbers which are 1 modulo q.

Theorem. *There are infinitely numbers $x \equiv a \pmod{q}$. Yeah, this is easy.*

Proof. Let's look at ψ characters of $(\mathbf{Z}/m\mathbf{Z}, +)$. Extend to Dirichlet character $\psi\colon \mathbf{N} \to \mathbf{C}$. Look at

$$\begin{aligned}\sum_{\psi} L(s,\psi) &= \sum_{\psi}\sum_{n=1}^{\infty}\frac{\psi(n)}{n^s} \\ &= \sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{\psi}\psi(n) \\ &= m\sum_{n=km}\frac{1}{n^s}.\end{aligned}$$

If there were finitely many $n \equiv 0 \pmod{m}$, then the right hand side would need to be finite. However, we can show rather easily that

$$\lim_{s\to 1^+}\sum_{\psi} L(s,\psi) = \infty,$$

and so there must be infinitely many n. The obstacles we'll face are

- Actually analyze the above sum;
- We want to sum over only primes which are congruent to 1 modulo q;
- We want to restrict our attention to things that are only relatively prime to q.

■

Convergence of L-functions

Let χ be a character of $G \simeq (\mathbf{Z}/q\mathbf{Z})^\times$. Assume that $\chi \neq \chi_0$. We know that

$$\sum_{x\in G}\chi(x) = 0 \implies \sum_{x=0}^{q-1}\chi(x) = 0, \qquad \text{(by orthogonality)}$$

so consider

$$\sum_{n\le x}\chi(n) = \sum_{n\le kq}\chi(n) + \sum_{kq+1}^{x}\chi(n) \le \varphi(q),$$

where the first term must be 0, and in the latter, there are at most $\varphi(q)$ summands which are relatively prime to q. This implies that the L-functions always converge.

Problem 14.1 (Homework)**.** Let $f(n)$ be a monotonically decreasing positive function. Then $\sum_{n=M}^{N} f(n)\chi(n) \leq 3\varphi(q)f(M)$. **Hint:** We know that χ is a periodic function. Use summation by parts.

Corollary 14.2. *If χ is not χ_0 and $s > 0$ then*

$$L(s,\chi) = \sum \frac{\chi(n)}{n^s}$$

converges.

Proof. Use the homework problem to get that

$$\left| L(s,\chi) - \sum_{n \leq x} \frac{\chi(n)}{n^s} \right| \leq \frac{3\varphi(q)}{n^s},$$

which goes to zero. ∎

Since this function converges, we get an Euler product

$$\begin{aligned} L(s,\chi) &= \prod_{p \text{ prime}} \left(1 + \frac{\chi(p)}{p^2} + \frac{\chi(p^2)}{p^{2s}} + \cdots\right) \\ &= \prod_{p \text{ prime}} \left(\frac{1}{1 - \chi(p)/p^s}\right). \end{aligned}$$

In particular,

$$L(s,\chi_0) = \zeta(s) \prod_{p|q} \left(1 - \frac{1}{p^s}\right).$$