Notes for Cryptography

Professor Brian Sittinger

5/2/16

1 Introduction

The last homework has been put out.

2 Number Field Sieve

A technique to factor large composite numbers. Given a number n which we wish to factor chose a degree d depentent on n,

$$d \approx \sqrt{\frac{\log n}{\log \log n}}$$

in practice. Let

$$m = \lfloor \sqrt[d]{n} \rfloor$$

an expand n in base m

$$n = m^d + a_{d-1}m^{d-1} + \cdots + a_0$$

Let α be a root of this (non-rational). See the notes from class. Ergo, we may work in $\mathcal{O}(\alpha)$.

A number is smooth if it factors into small primes. So we find some α in $\mathcal{O}$ such that $\langle \alpha \rangle$ is smooth in $\mathcal{O}$ and $h(\alpha)$ is smooth in $\mathbb{Z}$. We have factor bases a list of permissible primes and units.

The first list on the notes is of factor bases for $\gcd(a, b) = 1$ What we want is

$$\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathcal{O}$$

such that

$$\langle \alpha_1 \alpha_2 \ldots \alpha_r \rangle = \beta^2 \in \mathcal{O}$$

With this, we now use the trick below: if we suppose that

$$x^2 \equiv y^2 \mod n$$

$$x \not\equiv \pm y \pmod{n}$$

Then $\gcd(x-y, n)$ is a factor of n.

And note that

$$\gcd(1807-38, 2501) \equiv 61$$

Which is prime, and a prime factor if 2501.

3 Dirchlet's Theorem (Primes in Arithmetic Progression)

For $m \in \mathbb{N}_{>1}$, let $\gcd(a,m) = 1$. There are infinirely many primes congruent to $a \pmod{m}$.

Proof (stretch): We'll show (the stronger statement) that

$$\lim_{s \to 1^+} \frac{\sum_{prime p} p^{-s}}{\sum_p p^{-s}} = 1/\phi(m)$$

This is known as the Dirchlet density. A non-zero Dirchlet density implies that $|A| \Rightarrow \infty$. A corrolary Moreover, there is asymptoticall an equal number of primes in any congruence class $a \pmod{m}$, where $\gcd(a,m) = 1$.

Some background material (Fourier Analysis) let $G = (\mathbb{Z}_m)^*$. Define

$$G^* = \{\chi : G \to \mathbb{C}^*\}$$

The dual group (set of "Dirchlet Class" modulo m). A fact:

$$|G^*| = \phi(m)$$

An example,

$$\mathbb{Z}_5^*$$

We use $\langle 2 \rangle$ χ is completely determined by value sr 2. 2 Has order $4 = \phi(5)$.

$$\chi(2) \in \mathbb{C}^*$$

order divisor of 4. So, $\chi(2) = i^k$ for some $k \in \{1,2,3,4\}$.

So, now we apply Fourier. We have orthagonality relations, which are usually represented by sins and coss. So what do our orthagonality relations look like here.

$$\sum_{\text{gcd}} \chi(g) = \begin{cases} \phi(m) = |G| & \text{if } \chi = 1 \\ 0 & \text{if } \chi \neq 1 \end{cases}$$

$$\sum_{\chi \in G^*} \chi(g) = \begin{cases} \phi(m) = |G^*| & \text{if } \chi = 1 \forall \text{ fixed } \chi \in G^* \\ 0 & \text{if } g \neq e \end{cases}$$

Definition, Fourier Series of $f : G \to \mathbb{C}$. $s_f(x) = \sum_{\chi \in G^*} \hat{f}(\chi)\chi(x)$

$$\hat{f} = \frac{1}{\phi(m)} \sum_{g \in G} f(g)\chi(g^{-1})$$

$\hat{f}: G^* \to \mathbb{C}$. The Fourier coefficient (transform of f). I need $s_f(g) = f(g) \forall g \in G$ via orthagolan relation.

Proof part 1: Let $f : G \to \mathbb{C}$ be the characteristic function $f(x) = \begin{cases} 1 & x \equiv a \pmod{m} \\ 0 & x \not\equiv a \pmod{m} \end{cases}$
Then forall $\chi \in G^*$ we have,

$$\hat{f}(\chi) = 1/\phi(m) \sum_{x \in G} f(x)\chi(x^{-1}) = \frac{1}{\phi(m)}\chi(a^{-1})$$

so, $s_f(x) = f(x)$ reduces to

$$\sum_{\chi \in G^*} (\frac{1}{\phi(a)}\chi(a^{-1}))\chi(x) = \frac{1}{\phi(m)} \sum_{\chi \in G^*} \chi(a^{-1}x) = \begin{cases} 1 & x \equiv a \pmod{m} \\ 0 & \text{else} \end{cases}$$

Now, we consider

$$\sum_{p \equiv a \pmod{m}} p^{-s}$$

Key idea: use f to take the sum over all primes p instead of some primes. Then replace f with its Fourier Series. Then,

$$\sum_{p \equiv a \pmod{m}} p^{-s} = \sum_p f(p)p^{-s} = \sum_p \left(\frac{1}{\phi(m)} \sum_x \chi(pa^{-1}) \right) p^{-s} = \frac{1}{\phi(m)} \sum_\chi \chi(a^{-1}) \sum_p \chi(p)p^{-s}$$

Define $L(z, \chi) = \sum \frac{\chi(n)}{n^s} := \prod_p (1 - \chi(p)p^{-s})^{-1}$. At this point we can now use the fundamental theorem of Algebra. Note that

$$\chi = 1 \Rightarrow L(s, 1) = \zeta(s)$$

So,

$$\log L(s, \chi) = -\sum_p \log(1-\chi(p)p^{-s}) = \sum_{k=1} k^{-1}\chi(p^k)p^{-ks} = \sum_{k=1} \chi(p)p^{-s} + \sum_{k \geq 2} k^{-1}\chi(p^k)p^{-ks}$$

log is base e. We now use the traingle inequality (we know $s, k > 1$).

$$< \sum_p \sum_{k=2}^{\infty} = 1^{-1}1p^{-k}$$

$$= \sum_P \frac{1}{p(p-1)}$$

$$\leq \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1$$

By the use of a telescoping sum!

In summary,

$$\sum_{p\equiv a \pmod m} p^{-5} = \frac{1}{\phi(m)}\left[\sum_{\chi}\chi(a^{-1})\log L(\chi,s)\right] + O(1)$$

We show that the right hand side approaches infinity as $s \to 1^+$. Facts true for $\chi = 1$. So $\zeta(s)$ has a simple pk at $s = 1$ with residue 1.

$$\zeta(s) = \frac{1}{s-1} + \text{analytic stuff}$$

For all $\chi \neq 1$

$$L(1,\chi) \neq 0$$

and finite. Then

$$\sum_{p\equiv a(m)} p^{-s} = \frac{1}{\phi(m)}\left[\sum_{\chi}\chi(a^{-1})\log L(s,\chi)\right] + O(1)$$

$$= \frac{1}{\phi}\left[\log(\zeta(s)) + \sum_{\chi\neq 1}\chi(a^{-1})\log(L(\chi,s))\right] + O(1)$$

$O(1)$ is Big O notation.

$$\frac{1}{\phi(m)}\log\left(\frac{1}{s-1}\right) + O(1)$$

Now we apply this back in the original statement, and take the limit.

There's also something called the natural density.

$$\pi_A(x)/\pi(x)$$

Where π is the number of primes up to x. We can take the limit as x approaches infinity. The reasoning behind this is

$$\pi_A(x) = \sum \zeta = \sum f(p)1$$

4 Homework

Part 1b and c are linked - we use part be to do part c. What we're trying to do is

$$\left(\frac{a}{p}\right) = 1$$

for half of $a \in \{1, \ldots, p-1\}$

$$a \pmod p$$

So for a given a, there are an infinite number of ways to have p. Email the professor if stuck!