Notes for Cryptography

Professor Brian Sittinger

1 Textbooks

Homework is DUE NEXT MODNDAY Supplemental Books:
Daniel Marcus, Number Fields. Jurgan Neukirch, Algorithmic Number Theory. But the primary textbook is "Algebraic Number Theory and Fermat's Last Theorem" by Ian Stewart and David Tall 4th edition though the edition isn't important.

2 Office Hours

Officially 12–1pm. But actually from around 10:45–1:30pm. Another break is in his schedule after DST around 2:45pm.

3 Assignments

There will be two take home exams. There will be a final exam and a final project. In extenuating circumstances email the professor. Around the 6th and 12th weeks we will have midterms. One will be around easter break. `http://faculty.csuci.edu/brian.sittinger` Has all the info. First HW is up tomorrow morning.

4 Introductions

Ian - highschool. Math95 Su persoky teaching math 94 Mohita Alex MC beurm First year math Alex - 2 years - teaches Michel luis - 3rd semester Merina math95 last semester Mira - last semester math 95 Moorpark Highschool - 3/4th semester Dana - teaches precalc Vicne Fergusson math 95 - 3rd semester Maria - teaching math 95 Jennifer Lu Not teaching math Ivan first semester math 95 Matt CS, Softwaree Cara David second semseter - Vijay CS - 3rd sem Dhruv Mark George Calc 1 Kevin

5 Crash Course Review of Elementory Number Theory

Number theory is sometimes called Arithmetic. We then go into the basic sets. Number theory is the study of the proprertyies of $\mathbb{Z}$ or ($\mathbb{N}$). The multiplicative structure of $\mathbb{Z}$ is of main focus to us. We say that $a|b$ (a divides b) iff there exists $c \in \mathbb{Z}$ such that $a = bc$. Now let $a, b, c \in \mathbb{Z}$. Then

- $a|b \Rightarrow a|bc$
- $a|b, a|c \Rightarrow a|(b+c), a|bc$ More generally

$$a|mb + nc \forall n, m \in \mathbb{Z}$$

- $1|a, a|0$
- A Prime or an irreducible number is one that is only divided by 1 and itself. A prime will have exactly 2 prime factors - so 1 is not prime. An integer not equal to ± 1 with more than 2 prime factors is composite.

The fundamental theorem of Arithmetic. Every integer not in $\{0, -1, 1\}$ has a unique prime factorization (up to order and signs).

We define the GCD (Greatest Common Divisor) as the largest positive integer which divides all the arguments. LCM is the least common multiple, is the smallest positive integer which is a multiple of all arguemnts. For the GCD we use the minimum of each power of a factors and the LCM we use the maximum for each power of factors. If the GCD of two numbers is 1, we say that they are coprime or relatively prime. If any subset of the integers have the property that any two of them are relatively prime, that subset is "pairwise relatively prime." 3, 5, and 9 are relatively prime, but not pairwise relatively prime.

Some properties:

- if $a|b,$ and $c|b$ then, $\gcd(a, c)|b$.
- Let p be a prime. Then if $p|ab$ Then

$$p|a \text{ or } p|b$$

  This is an alternative definition for primality.

6 Modular Arithmetic

Fix $m \in \mathbb{N}_{>1}$. Given $a, b \in \mathbb{Z}$ we write

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

to say that

$$m|a - b$$

That is a and b have the same remainder when divided by m. And if

$$a \equiv 0 \pmod{m}$$

$m|a$ since there exists some $k \in \mathbb{Z}$ such that

$$a = 0 + km$$

6.1 Solving Congruences

Addition, and multiplication over a modulus is simple. Division is possible when m is prime. Then $\mathbb{Z}_p$ is a field. If

$$ac \equiv dc \pmod{m}$$

Then

$$a \equiv d \pmod{\frac{m}{\gcd m, c}}$$

However, 4 has no inverse mod 12 and

$$4x \equiv 8 \pmod{12}$$

has the solution

$$x \equiv 2 \pmod{3}$$

or

$$x \equiv 2, 5, 8, 11 \pmod{12}$$

A new example.

$$x^2 \equiv 5 \pmod{11}$$

Note that

$$5 \equiv 16 \pmod{11}$$

And since 11 is prime, this has exactly 2 solutions: ± 4. This can be rewritten as

$$11|(x+4)(x-4)$$

as expected. Also, remember that

$$x \overset{\equiv}{} 6 \pmod{11}$$

Has no solution since

$$0^2, (\pm 1)^2, (\pm 3)^2, (\pm 4)^2, (\pm 5)^2$$

goes up to 5.

6.2 Diophantine Equations

Consider

$$x^2 + y^2 = 4027$$

It has no integer solutions. Consider this mod 4.

$$x^2 + y^2 \equiv 3 \pmod 4$$

However, this has no solution since

$$0, (\pm 1), (\pm 2)$$

fails.

6.3 Fermat's Little Theorem

If the GCD of a and p is 1, and p is prime, then

$$a^{p-1} = 1 \pmod p$$

This is useful for reducing large exponents to something managable. For example

$$3^{105} \mod 13$$

is equivalent to

$$\left(3^{13-1}\right)^8 \cdot 3^9 \equiv 1 \pmod{13}$$

6.3.1 Euler Phi Function

Let $\phi(n)$ be the number of integers from 1 to n inclusive that are relatively prime to n. Then if

$$\gcd(a, m) = 1, a^{\phi(m)} \equiv 1 \mod m$$

And we get Fermet's Little theorem again when m is prime.

Another example

$$47^4 2 \pmod{100}$$

47 and 100 are coprime, so

$$\phi(100) = \frac{\phi(2^2)}{2} \cdot \frac{\phi(5^2)}{20}$$

6.4 Wilson's Theorem

p is prime is equivalent to

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

6.5 Chinese Remainder Theorem

Suppose that $m_1, \ldots, m_k$ are pairwise relatively prime. Then $x \equiv a_i \mod m_i$ for all $i \in [1, k]$ has a unique solution mod $m_1 m_2 \ldots m_k$. Or

$$\mathbb{Z}_{m_1 \ldots m_k} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$$

An example,

$$x \equiv 1 \mod 2$$
$$x \equiv 2 \mod 3$$
$$x \equiv 3 \mod 11$$

Then

$$x \equiv 5 \mod 6$$
$$x \equiv 3 \mod 11$$

So

$$5 + 6k = 3 \mod 11$$
$$k = 7 \mod 11$$