CS174 Discussion Section Notes #7 **Hao Zhang** nhz@eecs.berkeley.edu

Disclaimer: *These notes have not been subjected to the usual scrutiny for formal publications. They are to be used only for the class.*
Outline:

1. A few results from Number Theory

1 A few results from Number Theory

In class, we've seen an application of number theory when we did the fingerprinting based on integers modulo p, where p is a prime number. That example gives the flavor of how number theory, a relatively obscured area in mathematics, can be used to design efficient practical algorithms. A well-known application is cryptography. Most of today's cyphers are based on number theoretic techniques. For instance, using tools from number theory, one can prove that the problem of factoring a integer into primes is NP-Hard. Based on this knowledge, one can design codes that are vulnerable only if there's a polynomial-time algorithm to factor integer into prime numbers. Because it is conjectured that P$\neq$NP, such an algorithm is unlikely to exist.

Number theory is a rich and diverse field. Here, I will introduce a few common and useful results that show up often in the analysis of randomized algorithms.

We'll start with the idea of modulo, which is central to all of number theory. Given an integer n, consider all possibilities of an integer modulo n, that is, $\{0,1,2,...,n-1\}$. Denote this set by Z_n and redefine addition as usual addition but modulo n (for example, $n-1+n-1=2\times n-2=n-2 \pmod{n}$). And change the notion of multiplication in the same way (so that $(n-1)\times(n-1)=n^2-2\times n+1=1 \pmod{n}$).

Now we have a set Z_n with associated operations $+$ and $\times$, where everything is $\pmod{n}$. If n is a prime $n=p$, then this defines what is so called a "field". (Other examples of fields include the set of real numbers (R) or complex numbers (C) under the usual notion of $+$ and $\times$.) Analogous to other fields, the field of Z_p gives us a framework to study various mathematical objects such as identities as well as equations involving unknowns. For instance, we observe the fact that when $n=p$ is prime

$$(n-1)!+1=0 \pmod{n}$$

This identity actually holds if and only if n is a prime p and is called the Wilson's theorem. We can also ask questions about equations, say, quadratic equations of the form

$$x^2=-1 \pmod{p}$$

We want to know when this equation has a solution in Z_p. (Compare this with quadratic equations in R.) As it turns out, we have pretty neat description of the solutions for the kind of quadratic equation above. And you will be able to see how this works later on.

For primes, it is also known that

$$2^p - 2 = 0 \pmod{p}$$

This identity is often mentioned in algorithm textbooks and is the Fermat's Little Theorem. It is called Little Theorem as opposed to Fermat's Last Theorem (which was a celebrated conjecture until a proof was found by Andrew Wiles a few years ago).

Here is a proof for the Little Theorem: write 2=1+1 and expand $(1+1)^p$ into a sum of binomial coefficients:

$$(1+1)^p = \sum_{i=1}^{p} \binom{p}{i}$$

The first and last summands are both 1s ($\binom{p}{0} = \binom{p}{p}$=1). Any of the rest of the summands can be written as:

$$\binom{p}{i} = \frac{p(p-1)..(p-i+1)}{12...i}$$

which has a factor of p in the numerator that can't possibly be affected by anything in the denominator (since p is only divisible by itself). Therefore, all such terms are divisible by p. So we are left with only the first and last term. Hence, $2^p - 2$ is divisible by p. ■

The Little Theorem can be generalized to $a^p - a = 0 \pmod{p}$. You may try to prove this as an exercise (hint: multi-nomial coefficients)

An elementary proof such as above doesn't carry us very far in the realm of number theory. For deeper results, we need more advanced machinery, esp. notions from abstract algebra. A very useful and intuitive conceptual model is the notion of "cyclic group", which we will learn after the following preliminaries.

Suppose $n = p$ is a prime. As it turns out, if I take the element 0 out of Z_n. The rest of the elements form a set $Z_n^* = \{1, 2, ..., n-1\}$ which is closed under division (recall that neither R or C is closed under division: $\frac{1}{0}$ remains undefined ever since elementary school). Such a set is called "multiplicative group", as it is very friendly to the operation of multiplication and the inverse: division.

Moreover, a theorem says that Z_n^* is a cyclic group, meaning that there exists an element $w \in Z_n^*$ such that

1. $w^{n-1} = 1$, where $n-1$ equals the cardinality of Z_n^*.
2. The set of powers of w: $\{w, w^2, w^3, ..., w^{p-1}\}$ generates all the elements in Z_n^*. w is (naturally) called a "generator".

For example, let $p = 7$, then the number 3 is a generator: the powers of 3 are $3^1 = 3, 3^2 = 9 = 2, 3^3 = 3^2 \times 3 = 2 \times 3 = 6, 3^4 = 6 \times 3 = 18 = 4, 5, 1$, that is $\{3, 2, 6, 4, 5, 1\}$ and is Z_7^*.

The fact that Z_n^* is a cyclic group with a generator is far from trivial(a proof can be found in a number theory or abstract algebra textbook). However, the fact itself is very handy to use to prove other things.

For example, the Fermat's Little Theorem follows easily: for any $a \neq 0$, we now know that a is some power of g, where g is the generator, write $a = g^k$, then

$$a^{p-1} = (g^k)^{p-1} = (g^{p-1})^k = 1^k = 1 \pmod{p}$$

(recall $g^{p-1} = 1$). Hence, $a^{p-1} - 1 = 0 \pmod{p}$. The remaining case is when $a = 0$, then $a^p - a = a(a^{p-1} - 1)$ clearly is divisible by p. ■

We can also study the solution structure of the quadratic equation we had earlier:

$$x^2 = -1 \pmod{p} (*)$$

In the field of integers, we had the familiar notion of squares as the set of integers $\{1, 4, 9, 16, ...\}$. A similar notion of "quadratic residues" can be defined for the field of Z_n, which is the remainder of integer squares mod n. For example, if n is a prime, say, $n = 7$, then the quadratic residues are:

$$\{1, 4, 9, 16, ...\} \mod 7 = \{1, 2, 4\}$$

You may verify the fact that there is always a number of $\frac{p-1}{2}$ quadratic residues. In fact, a deeper result holds: the quadratic residues are even powers of the generator, that is, $\{g^2, g^4, ..., g^{p-1}\}$. Look back at equation (*): it really asks whether -1 belongs to the set of quadratic residues.

If -1 belongs to the set, that means there exists a power of g: $g^k = -1$. Hence, $(g^k)^2 = g^{2k} = 1$. Since we know the only power of g that equals 1 is $g^{p-1} = 1$, this implies $2k = p - 1$, namely $k = \frac{p-1}{2}$. Now, recall the quadratic residues are even powers. So g^k belongs to the set of quadratic residues only if k is even. This happens only when $p = 4n + 1$ for some n.

On the other hand, similarly one can show that the converse is true: when $p = 4n + 3$, the set of quadratic residues does not include -1.

This gives us the neat statement that the equation (*) has a solution iff $p = 4n + 1$. ■

However, the tools from abstract algebra is not the swiss army knife for everything. The field of number theory involves many diverse techniques other than those from abstract algebra.