2004-2005 INTRODUCTION: PRIMES

Die ganze Zahl schuf der liebe Gott, alles Übrige ist Menschenwerk.

Leopold Kronecker, circa 1850

1. introduction to the 2004-2005 utah math circle

Sometimes we get lucky. For instance, if you haven't thought very much about it there is no reason to believe that the ratio of the circumference to the diameter of a circle should be the same for every circle. The fact that it is a constant — the constant π — is surprising. Even if this is not surprising to you, the fact that π turns out to be an interesting number — as opposed to 3 or 22/7 or $\sqrt{10}$ — surely must be surprising. For instance, π is not rational (i.e. it is not the solution of an equation of the form $ax - b = 0$ for whole numbers a and b). In fact, π is even transcendental in the sense that there is no polynomial $p(x)$ with integer coefficients such that π is the solution to $p(x) = 0$. So we should feel very lucky that such an interesting contant is given to us essentially for free. It therefore should not be surprising that π shows up everywhere in mathematics — even in places you might not expect it.

What was Kronecker talking about in his famous quote? He might have meant following. We all have fingers, so we learn to count, and hence are led to the positive whole numbers and the concept of addition. Subtraction is the inverse of addition, and so we are led to zero and the negative whole numbers. Multiplication is iterated addition and division is the inverse of multiplication. This leads up to the rational numbers. And so on. Man continues in this way building up all of mathematics[1].

Again we get lucky: at almost the very first step of Kronecker's scheme we are handed something extemely interesting. Once we have the notion of multipication (i.e. iterated addition), we can immediately define a prime number p to be a positive whole number for which there do not exist positive whole numbers a and b strictly smaller than p such that a times b equals p. Because this is such a simple definition, one might expect it to be a boring concept. Here we get another surprise: trying to understand prime numbers present some of the most interesting questions in all of mathematics.

The focus of the Utah Math Circle is two-fold. First we seek to understand simple, natural mathematical definitions, and (more importantly) the deeper theory they suggest. The second focus is to use that kind of theory to solve interesting problems. In the next two weeks, we'll focus on the following problem: given an integer n, how can we efficiently decide if n is prime. (Of course one way is to divide n by all numbers smaller than n and see if we ever find one for which this division doesn't have a remainder. But this isn't very

[1]Actually the context of Kronecker's quote was far more polemic. He believed that the only "true" mathematical constructs were those based in the whole numbers, and denied the existence of transcendental numbers (like π, which was proved to be transcendental during Kronecker's lifetime).

efficient!) We'll also see the applications of this question to the kind of encryption that you encounter every day (perhaps without knowing it) when you use the internet.

2. MODULAR ARITHMETIC

This is a concept that all of you are already familiar with, but we'll spell it out carefully. Fix a positive integer n, suppose a is any integer. The *reduction of a modulo n* is defined to be the remainder, say r, that we get when we divide n by a. Of course we can always arrange for this remainder to be between 0 and $n-1$. With this convention in place, we write $a \equiv r \mod n$.

Now set $\mathbb{Z}/n = \{0, 1, \ldots, n-1\}$. We obtain a kind of addition on $\mathbb{Z}/n$: if $a, b \in \mathbb{Z}/n$ we can first add a and b together. The problem is that $a+b$ need not be in $\mathbb{Z}/n$ (since $a+b$ could be bigger than $n-1$). But if reduce $a+b$ modulo n we arrive back in $\mathbb{Z}/n$. We call this procedure addition modulo n. It eats two element of $\mathbb{Z}/n$ and spits out a single element of $\mathbb{Z}/n$.

Of course we can do the same thing with multitiplication replaced by addition. The resultis called multiplication modulo n. It also eats two element of $\mathbb{Z}/n$ and spits out a single element of $\mathbb{Z}/n$.

Exercise 2.1. Break for first sheet of exercises.

One reason we need fractions is so that for every $m \in \mathbb{Z}$ there exists a number l such that $ml = 1$. Of course we usually write $\frac{1}{m}$ or m^{-1} for l. But obviously we need to expand our scope from the integers to the fractions for this to make sense.

Exercise 2.2. When do we need "fractions" for $\mathbb{Z}/n$? [Discuss. Then break for first sheet of exercises.]

We are in a position to prove several famous theorems.

Theorem 2.3 (Fermat's Little Theorem)**.** *Fix a prime p. Then $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}/p$.*

Exercise 2.4. Is it important for p to be prime in the statement of Fermat's Little Theorem? (It turns out that there are infinitely many *composite* numbers n such that $a^n \equiv a \mod n$ for all $a \in \mathbb{Z}/n$. Such numbers are called Carmichael numbers. The first Carmichael number is 561.)

Here is another famous theorem.

Theorem 2.5 (Wilson's Theorem)**.** *Fix a prime p. Then $(p-1)! \equiv p-1 \mod p$*

Euler generalized Fermat's Little Theorem as follows. Suppose n is a not-necessarily-prime number. We know that there are some elements $a \in \mathbb{Z}/n$ for which a^{-1} doesn't exist. But we can still define

$$(\mathbb{Z}/n)^* := \{a \in \mathbb{Z}/n \mid a^{-1} \text{ exists } \}.$$

For instance, if $n = p$ is prime, we have

$$(\mathbb{Z}/p)^* = \{a \in \mathbb{Z}/p \mid a \neq 0\};$$

but in general $(\mathbb{Z}/n)^*$ will be quite a bit smaller than the nonzero elements of $\mathbb{Z}/n$. So we can define

$$\phi(n) = \text{ the number of elements of } (\mathbb{Z}/n)^*.$$

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

Exercise 2.6. Hand out the third installment of exercises. Discuss alternate definitions of $\phi(n)$ and the cyclic structure of $(\mathbb{Z}/p)^*$

Here is Euler's generalization.

Theorem 2.7 (Euler)**.** *For any $a \in \mathbb{Z}/n$, $a^{\phi(n)} \equiv 1 \mod n$.*

Exercise 2.8. Verify the theorem using the computations from the second installment of exercises. Make sure you see Fermat's Little Theorem as a special case of Euler's theorem.

3. A CRYPTROGRAPHIC TRICK

Suppose I want to send you a secret message. As a first step you and I would need to agree on a secret code. Then I can encrpyt the message using the secret code, mail it to you, and since we've both agreed on the code, you'll be able to decrypt the message and read its contents. If the message is intercepted, then since no one beside you and I know the secret code, the content of the message will be safe (assuming the code is a good one, which is another matter altogether).

So how can you and I devise a secret code? One option would be to meet in person. Clearly this is impractical. It turns out that there is a very clever trick using only the difficult of computing discrete logs (which me met in the exercises) and which makes it possible for you and me to agree on a secret code without every meeting. This trick was discovered in the 1970's (or in fact rediscovered) and ushered in new era of cyptography.

Agreeing on a secret code amounts to essentially picking a secret number. One option would be for me to pick a number and mail it to you. The mailing is obviously susceptible to interception, however, and is clearly inadequate. So instead you and I proceed as follows. We first pick two large numbers x and y. This choice doesn't have to be secret — we could post the values of x and y on a webpage, for instance. Then I pick a secret number, say A, known only to me. Meanwhile you pick another such secret number B known only to you. I compute $x^A \mod y$ (call the result A') and mail A' to you. We've seen in the exercises that

the computation of A' is easy. We've also seen that reconstructing A from knowing x, y and A is very hard. (This is the discrete log problem.) So even if A' gets intercepted, the value of A remains secure. Meanwhile, you compute $B' = B^x \mod y$ and mail B' to me. Again the actual value of B is secure.

Now comes the trick. I take your mail containing B' and compute

$$C_{\text{me}} = (B')^A \mod y.$$

Meanwhile you compute

$$C_{\text{you}} = (A')^B \mod y.$$

Since $B' = x^B \mod y$, then we see that

$$C_{\text{me}} = (x^B)^A \mod q = x^{BA} \mod q.$$

Likewise we see that

$$C_{\text{you}} = (x^A)^B = x^{AB} \mod q.$$

In other words,

$$C_{\text{me}} = C_{\text{you}}.$$

We have managed to agree on a secret number C is a manner that is perfectly secure! We can then use C as the basis of our secret code.

4. ANOTHER CRYPTROGRAPHIC TRICK

With out knowledge of Euler's Theorem in hand, we are in a position to understand one of the most widely used encryption schemes. I begin by choosing two enormous prime numbers p and q and a third number x subject only to the requirement that $p-1$, $q-1$, and x share no common factor. I multiply p times q and call the result, say N. I then post N and x on my webpage. Since N is an extremely large number and since we discussed in the exercises that factoring large numbers is hard, the actual values of p and q cannot be determined from the knowledge of N.

Now suppose you want to send me a secret message. You can convert any sequence of letters to numbers (in an obvious way), so it's enough for you to be able to send me a secret number, say M (for message). You go to my webpage and look up my posted values of N and x. Then you compute

$$M' = M^x \mod N.$$

We've seen how to do this efficiently in the exercises. Then you mail me M'. It's OK if M' gets intercepted, since (as we've discussed) its very difficult to reconstruct M from M'.

So now I have M' and I need to recover M from it using my secret knowledge of p and q (whose values are known to me and no one else). First I compute a new number, say y, so that

$$xy = 1 \mod (p-1)(q-1).$$

(Again we've seen how to do this in the exercises.) To say that $xy = 1 \mod (p-1)(q-1)$ means that

$$xy = 1 + k(p-1)(q-1) \tag{1}$$

for some k. We recognize that $\phi(N) = (p-1)(q-1)$. So now I compute

$$\begin{aligned}(M')^d \mod N &= (M^y)^d \mod N = M^{xy} \mod N \\ &= M^{1+k\phi(N)} \mod N = M \cdot (M^{\phi(N)})^k \mod N,\end{aligned}$$

where to get fro the first line to the second, I've used Equation (1) and the fact that $\phi(N) = (p-1)(q-1)$. From Euler's Theorem (Section 2) we know $M^{\phi(N)} = 1 \mod N$. Thus we conclude that

$$(M')^d = M \mod N.$$

In other words I've reconstructed your message M!

5. TESTING FOR PRIMALITY

In the previous section, we saw the importance of generating large prime numbers. So that motivates the following question: given n, find an efficient way to determine if n is prime. What does efficient mean in this context? Here is one measure. Suppose we have a procedure (running on a deterministic computer) that inputs an integer and spits out an answer "Yes" or "No" (as in "Yes, n is prime" or "No, n is not prime). Let T be the time it takes to run the procedure. Typically T will depend on the size of the input n. One may thus plot T versus n. This isn't quite what we want to do. Instead we want to plot T versus the *number of digits in* n. If we can find a polynomial p such that the graph of p is always bigger than this graph, then we say that the procedure P *runs in polynomial time*. To say that P runs in polynomial time is some measure of the efficiency of P.

Exercise 5.1. Break to discuss P versus NP.

Here is a procedure to determine whether n is prime. (Much of the forgoing exposition was lifted from another set of notes, "Is this number prime?" by Kiran Kedalaya available at http://mathcircle.berkeley.edu/BMC5/docpspdf/is-prime.pdf.)

Step 1. Pick a number $a \in \{1, 2, \ldots n\}$.

Step 2. Compute the gcd of n and a. If it's greater than 1, then stop: n is composite.

Step 3. Compute $a^{n-1} \mod n$. If it's not 1, then stop: n is composite.

Step 4. If test is inconclusive, then start over with a different choice of a.

Exercise 5.2. Does this procedure run in polynomial time? (For fast methods for Step 3, take a look at the exercises you did on the first sheet.)

What makes this test annoying is the existence of Carmichael numbers (see Exercise 2.4): they are composite, but always pass Step 3. Thus if we are given n which happens to be a Carmichael number, Step 2 must determine it's composite. But this really amounts to factoring n which (as we discussed in conjunction with Section 4 usually takes a very long time). So while each iteration of the test can be performed in polynomial time, if we had to run the test for all values of a, the cumulative procedure would probably not be polynomial.

Because it is such an old and natural questions, there is a rich theory of tests for primality. There are many fast algorithms to test whether a number is "probably" prime (that is that return a correct answer to the question "Is n prime?" most of the time). For many years, most people believed that there was no polynomial test for primality. About three years ago, a group of three Indian mathematicians (consisting of one professor, M. Agrawal, and two undergraduate students, N. Kayal and N. Saxena) shocked the mathematical community by producing a polynomial algorithm. Remarkably it essentially involved ideas no deeper than Fermat's Little Theorem (but, to be fair, an extremely clever application of thos ideas). Since then, a number of people have developed improved versions of the AKS algorithm.

EXERCISES I

1. Compute $2^{12} \mod 10$.
2. Compute $2^{24} \mod 10$.
3. Compute $2^{103} \mod 10$.
4. Compute $5^{103} \mod 103$.
5. Compute $10^{103} \mod 103$.
6. Compute $2^{561} \mod 561$.
7. Compute $3^{561} \mod 561$.
8. Compute $6^{41} \mod 55$.

EXERCISES II

1. Consider $\mathbb{Z}/5$. For which a does $a^-]$ exist?

2. Consider $\mathbb{Z}/11$. For which a does a^{-1} exist?

3. Consider $\mathbb{Z}/55$. For which a does a^{-1} exist?

4. Consider $\mathbb{Z}/123$. For which a does a^{-1} exist?

5. What is the general formula for the number of a such that a^{-1} exists in $\mathbb{Z}/n$?

6. Suppose p and q are prime and another number x so that $p-1$, $q-1$, and x share no common factor. Prove that there always exists $y \in \mathbb{Z}/(p-1)(q-1)$ such that

$$xy = 1 \mod (p-1)(q-1).$$

EXERCISES III

1. Consider $\mathbb{Z}/7$. Shows that there exists some x such that for all $a \neq 0$,

$$a = x^n$$

for some n.

2. Repeat the previous exercise for $\mathbb{Z}/11$.

3. Repeat the previous exercise for $\mathbb{Z}/25$.

4. Repeat the previous exercise for $\mathbb{Z}/49$.

5. Is it important that 7, 11, 25, and 49 are either prime or prime squares?