REU 2006 · Apprentice · Lecture 3a

Instructor: László Babai
Scribe: Matthew Booth
Editor: Sourav Chakraborty

June 28, 2006. Last updated June 30, 12:40am
PROOF-READ BY INSTRUCTOR

The notes are for the first half of the apprentice lecture given on June 28, 2006.

3a.1 The Infinitude of Primes

One theorem which is thousands of years old is that the set of prime numbers is infinite.

Theorem 3a.1.1. (Euclid) *There are infinitely many primes.*

Proof. (From Euclid's *Elements.*) Assume that there were only finitely many, say $p_1, \dots, p_n$. Let $q = \Pi_1^n p_i + 1$.

So $p_i \not| q$ since $q \equiv 1 \pmod{p_i}$. But any integer larger than 1 has a prime factor, which is a contradiction since no prime divides q. □

Theorem 3a.1.2. *There are infinitely many primes of the form* $4k-1$ *(i. e.,* $\equiv -1 \pmod 4$*).*

Observation 3a.1.3. Every odd number is $\equiv \pm 1 \pmod 4$. So every prime other than 2 is $\equiv \pm 1 \pmod 4$. Examples: the primes $5, 13, 17, 29, 37$ are congruent to $1 \pmod 4$ while the primes $3, 7, 11, 19, 23, 31$ are congruent to $-1 \pmod 4$.

Proof of the theorem. Suppose there are only finitely many primes $\equiv -1 \pmod 4$, $p_1, \dots, p_n$. Let $A = p_1 \dots p_n$. If n is odd, then $A \equiv -1 \pmod 4$ because

$$p_1 \dots p_n \equiv \underbrace{(-1) \dots (-1)}_{n \text{ times}} = (-1)^n = -1 \pmod 4.$$

Hence $A + 4 \equiv -1 \pmod 4$.

Lemma 3a.1.4. *$A + 4$ must have a prime divisor* $\equiv -1 \pmod 4$.

Proof of lemma. Actually if $B \equiv -1 \pmod 4$ (where B is any integer), then B has a prime divisor $\equiv -1 \pmod 4$. This is because if $B = q_1 \dots q_t$ is the prime factorization of B and $q_i \not\equiv -1 \pmod 4$, then $q_i = 2$ or $q_i \equiv 1 \pmod 4$. But $q_i \neq 2$ because B is odd. So if none of the $q_i \equiv -1 \pmod 4$, all of the q_i would be congruent to $1 \pmod 4$ and hence $B \equiv 1 \cdots 1 \equiv 1 \pmod 4$, which would be a contradiction. □

Lemma 3a.1.5. $p_i \not| A + 4$.

Proof of lemma. Now, $p_i \big| A$. If $p_i \big| A + 4$, then $p_i \big| ((A + 4) - A)$, and so $p_i \big| 4$ which is a contradiction.

□

So we saw that $A + 4$ must have a prime divisor $\equiv -1 \pmod 4$ and it is not divisible by any of the finitely many primes p_i congruent to $-1 \pmod 4$. This is a contradiction.

So we have taken care of the case when the number n is odd. To take care of when n is even, we just put down one of our primes twice when we define A to get that A is a product of an odd number of primes and we apply the same argument.

□

A slicker proof. Let $M = 4 \cdot p_1 \cdots p_n - 1$. Now $M \equiv -1 \pmod 4$ and so

1. M must have a prime divisor $\equiv -1 \pmod 4$ (by the lemma above).

2. $p_i \not| M$ because $M \equiv -1 \pmod{p_i}$.

and we arrive at a contradiction.

□

3a.2 Primes and Sums of Squares

Now we want to consider when we can write a prime number as the sum of two squares (i. e., $p = a^2 + b^2$). Let's start by looking at some examples.

Note that 5, 13 and 17 can be written as (a^2+b^2): $5 = 2^2+1^2, 13 = 2^2+3^2$ and $17 = 4^2+1^2$. But $3, 7, 11, 19$ cannot be expressed in that form.

Theorem 3a.2.1. (Fermat, Euler) *A prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$ or $p = 2$.*

We shall not prove this remarkable theorem today but we shall make the first steps towards understanding the problem.

One of the most useful "little" results of number theory is Fermat's "little" theorem.

Theorem 3a.2.2 (Fermat's little Theorem). *If p is a prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod p$.*

Proof. We invoke a counting theorem that was proved in the previous problem session: the number of necklaces with p beads, made of a kinds of beads, is $\frac{a^p-a}{p} + a$. (Two necklaces that are rotations of each other are considered the same.) So this number must be an integer. Hence $p \big| a^p - a$. But $a^p - a = a(a^{p-1} - 1)$. So since by assumption $p \not| a$, we have that $p \big| (a^{p-1} - 1)$ whence $a^{p-1} \equiv 1 \pmod p$.

□

Theorem 3a.2.3. *If p is prime and $p \equiv -1 \pmod 4$ then $p \neq a^2 + b^2$ for any integers a and b.*

Proof.

Question 3a.2.4. What is $a^2 \pmod 4$?

If a is even, then a^2 is divisible by 4 and so $a^2 \equiv 0 \pmod 4$. If a is odd, then both $a-1$ and $a+1$ are even and so $a^2 - 1 = (a-1)(a+1)$ is divisible by 4 and so $a^2 \equiv 1 \pmod 4$. So for all a, we have that a^2 is congruent to 0 or $1 \pmod 4$. So $a^2 + b^2$ is congruent to $0, 1$, or $2 \pmod 4$. So $a^2 + b^2 \not\equiv -1 \pmod 4$ and we have proven the theorem. □

Now there are numbers congruent to $1 \pmod 4$ which are not the sum of two squares (an example is 21). However, it turns out that every *prime* of that form is the sum of two squares.

Question 3a.2.5. Can $p \mid a^2 + b^2$, where p is a prime which is $\equiv -1 \pmod 4$?

Well, if $p \mid a$ and $p \mid b$, then of course it does, but that seems like cheating. So let's revise our question.

Question 3a.2.6. If $p \nmid a$ and $p \nmid b$, and $p \equiv -1 \pmod 4$, then can $p \mid a^2 + b^2$?

Suppose $p \mid a^2 + b^2$. If $p \nmid a$, then $p \nmid b$ (so we don't need to assume that p does not divide both of them, but only one of them). And we have that $a^2 \equiv -b^2 \pmod p$.

Exercise 3a.2.7. If there exists intergers a, b such that $a^2 \equiv -b^2 \pmod p$, then $p \not\equiv -1 \pmod 4$. [*Hint: Use Fermat's Little Theorem*]

The following theorem is an immediate consequence of this exericse. (Why?)

Theorem 3a.2.8. *If* $\gcd(a, b) = 1$, *then $a^2 + b^2$ has no prime divisors* $\equiv -1 \pmod 4$.

A consequence of this is the following theorem.

Theorem 3a.2.9. *There are infinitely many primes* $\equiv 1 \pmod 4$.

Proof. Assume there are only finitely many primes $\equiv 1 \pmod 4$, say $p_1, \cdots, p_n$. Let $A = p_1, \cdots p_n$. We want to find a number of the form $A^2 + b^2$ where b is a (hopefully small) integer such that

1. $A^2 + b^2$ is not divisible by any of the p_i
2. $A^2 + b^2$ has at least one prime divisor which is $\equiv 1 \pmod 4$. (In fact it will end up having all prime divisors $\equiv 1 \pmod 4$.)

Then we would have a contradiction. Now, $A^2 + 1^2$ doesn't give us quite what we want since it is an even number and hence is divisible by 2. But we could use $A^2 + 2^2$. Alternatively, we could use $(2A)^2 + 1^2$ and get what we want as well. □

Theorem 3a.2.10. *If $a^2 \equiv -b^2 \pmod p$, and $p \nmid a$, and p is an odd prime then $p \equiv 1 \pmod 4$.*

Proof. $a^{p-1} \equiv 1 \pmod p$. On the other hand,

$$1 \equiv a^{p-1} = (a^2)^{\frac{p-1}{2}} \equiv (-b^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}(b^2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} b^{p-1} \equiv (-1)^{\frac{p-1}{2}} (\operatorname{mod} p).$$

So $1 \equiv (-1)^{\frac{p-1}{2}} \pmod p$.

If $p \equiv -1 \pmod 4$, then $(-1)^{\frac{p-1}{2}} = -1$ since $\frac{p-1}{2}$ would be odd. But if $1 \equiv -1 \pmod p$, then $p = 2$, which is a contradiction since $2 \not\equiv -1 \pmod 4$. □

3a.3 Quadratic Residues

Definition 3a.3.1. If p is a prime, then a is a *quadratic residue mod p* if $p \nmid a$ and there is an x such that $x^2 \equiv a \pmod p$.

Definition 3a.3.2. If p is a prime, then a is a *quadratic nonresidue mod p* if there is no x such that $x^2 \equiv a \pmod p$.

Exercise 3a.3.3. *There are $\frac{p-1}{2}$ quadratic residues mod p (and hence $\frac{p-1}{2}$ nonresidues mod p). (Note: we are counting* residue classes, *i. e., all numbers that are congruent to a particular number mod p count as one number.)*

Question 3a.3.4. When is -1 a quadratic residue?

Exercise 3a.3.5. *If p is a prime and $p = a^2 + b^2$, then -1 is a quadratic residue mod p.*

Exercise 3a.3.6. *If $p \equiv -1 \pmod 4$, then -1 is a quadratic nonresidue mod p. [*Hint: this should be easy after today's class.*]*

Experiment 3a.3.7. *When is 2 a quadratic residue mod p? [Try to figure it out for primes less than 100 and make a conjecture.]*