MATH 115, SUMMER 2012
LECTURE 6

JAMES MCIVOR

Last time:

- Euler's Thm (Fermat's little Thm as special case): If $p \not| a$, then $a^{p-1} \equiv 1 \mod p$. - Wilson's Thm: $(p-1)! \equiv -1 \mod p$.

Today we get another famous Thm of Fermat

Theorem 1 (Fermat's Theorem on Sums of Squares)**.** *Let n be any positive integer, and write its prime factorization as*

$$n = 2^k \cdot \prod p^{\alpha(p)} \prod q^{\beta(p)},$$

where the primes p are congruent to 1 mod 4 and the primes q are congruent to 3 mod 4. Then n can be written as a sum of two squares if and only if all $\beta(q)$ are even.

We prove it using the following five facts. Not that there are three types of primes: 1) p=2, 2) $p \equiv 1$ mod 4, and 3) $p \equiv 3$ mod 4. The idea is to work out whether each of these types of prime can be written as sums of squares, and then put this altogether using prime factorization.

(1) (Seemingly random but useful) Let p be an odd prime. Then $x^2 \equiv -1 \mod p$ has a solution if and only if either $p \equiv 1 \mod 4$ or $p = 2$.
(2) 2 can be written as a sum of squares $(1^2 + 1^2)$
(3) If p is an odd prime with $p \equiv 1 \mod 4$ then there are a, b such that $p = a^2 + b^2$.
(4) Let $q | a^2 + b^2$. If $q \equiv 3$ mod 4 then $q | a$ and $q | b$.
(5) If m and n can be written as sums of squares, so can mn.

1. Proof of Thm using 1-5

For the "if" direction, we know that the p's can be written as sums of squares. So can the 2's: $2 = 1^2 + 1^2$. The q's, as we saw, cannot; but trivially $q^2 = q^2 + 0$. So each piece of the factorization can be written as a sum of squares; the lemma above tells us that therefore n can be.

For the "only if" direction, suppose $n = a^2 + b^2$. For each of the primes q, since $q | n$, we get that $q | a$ and $q | b$, so $q^2 | (a^2 + b^2) = n$. Thus each power of each q must be even (use induction - cancel q^2 and get a smaller integer)

2. Proofs of 1-5

Firstly, point 2 is obvious, and for part 5, use the formula $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ac + bc)^2$.

Proof of 1. $p = 2$ is clear, so first assume that $p \equiv 1 \mod 4$. This means that $\frac{p-1}{2}$ is even. Look at $(p-1)!$. Since $p-1$ is even, there are an even number of terms in the product. The middle two are $\frac{p-1}{2}$ and $\frac{p+1}{2}$. Break up the product like this:

$$(1 \cdot 2 \cdots \frac{p-1}{2})((p-1)(p-2)\cdots\frac{p+1}{2}),$$

and group the two first terms together, then the second two, and so on, giving

$$(1\cdot(p-1))(2\cdot(p-2))\cdots(\frac{p-1}{2}\frac{p+1}{2})$$

Now the first term is congruent to -1, the second to -4, and in general the ith pair is congruent to $-i^2$. Applying Wilson's Thm we have[1]

$$-1 \equiv (p-1)! \equiv \prod_{i=1}^{\frac{p-1}{2}}(-i^2) = \pm(\frac{p-1}{2}!)^2.$$

On the right, the ± is actually + under our assumption that $p \equiv 1 \mod 4$. Thus the solution is sitting right there: $x = \frac{p-1}{2}!$. This proves one direction.

Now assume instead that $x^2 \equiv -1 \mod p$ has a solution. Take $\frac{p-1}{2}$st powers of both sides, and use Fermat. You get $\pm 1 \equiv 1 \mod p$, where the ± is determined by whether $\frac{p-1}{2}$ is even or odd. To avoid a contradiction, it must be even, which is the same as saying $p \equiv 1 \mod 4$. □

Proof of 3. - see textbook - I gave that exact argument. □

Proof of 4. We reason by contradiction. Suppose without loss of generality that p doesn't divide a. Then a has an inverse mod p, call it a'. Since p divides $a^2 + b^2$, we have $a^2 + b^2 \equiv 0 \mod p$. Multiplying by a'^2 gives $(a'b)^2 \equiv -1 \mod p$. But we saw above (Prop 3) that this has a solution if and only if $p \equiv 1 \mod 4$[2] This is a contradiction, so $p|a$. □

3. Zagier's One-Sentence Proof of Point 3

Rather than give the proof from the book, I initially planned to use an incredibly short proof by number theory powerhouse Don Zagier, famously known as the "one-sentence proof". At the last minute I opted to give the proof above instead (following your text), but in case you're interested, below is my write-up of this Zagier proof.

Theorem 2. *Let p be a prime that is congruent to 1 mod 4. Then there are integers a and b such that $p = a^2 + b^2$.*

This proof is not at first very intuitive - it's really just a clever trick, but on the other hand I don't find the proof in your book too intuitive either. I'll let you decide which you prefer.

Proof. Right off the bat, note that p is odd here. This means that the only possible a, b that will work must be such that one is odd and the other even, say a odd and b even. Now, rather than look at solutions (a, b) to the equation $a^2 + b^2 = p$, we look instead at the set of ordered triples of integers (a, b, c) for which $a^2 + 4yz = p$. Call the set of such triples S. This S is a finite set, since a, b, and c cannot be too

[1] The following formula we nicknamed in class "The Sneaky Wilson"

[2] Prop 3 has the hypothesis that p is odd. But this holds here since we assumed $p \equiv 3 \mod 4$.

large. Notice that if we have such a triple in which $b = c$, then the term $4bc$ can be written as $2b \cdot 2b$, and then we must have that a is odd. Thus pairs (a, b) satisfying $a^2 + b^2 = p$ are equivalent to triples (a, b, c) satisfying $a^2 + 4bc = p$ for which $b = c$.

Now triples (a, b, c) for which $b = c$ can be described as follows. Consider the function $f \colon S \to S$ which "swaps" b and c: $f(a, b, c) = (a, c, b)$. The triples we're interested are "fixed points" of this function, namely they're the triples for which $f(a, b, c) = (a, b, c)$. Now this function is what is called an involution: that's a function which, when you apply it twice, you get back the same thing, i.e., f^2 is the identity function on S. It turns out, that for any involution on a finite set, the number of fixed points is even if the size of S is even, and odd if the size of S is odd. The reason is that the subset of no-fixed points must be of even size, for each non-fixed point gets paired up with another distinct non-fixed point since it's an involution. So (size of fixed pt set) = (size of S) - (size of fixed non-fixed pt set), and subtracting off an even number doesn't affect parity.

We want to show that the number of fixed points of f is odd, since then it cannot be zero, so there is at least one solution. But the number of fixed points will have the same parity for any involution, so instead of determining the parity of f's fixed points directly, we look instead at the bizarre involution

$$g(a, b, c) = \begin{cases} (a + 2c, c, b - a - c) & \text{if } a < b - c \\ (2b - a, b, a - b + c) & \text{if } b - c < a < 2b \\ (a - 2b, a - b + c, b) & \text{if } a > 2b \end{cases}$$

Now one checks a) that this is really an involution on S, and b) that it has only one fixed point, namely $(1, 1, \frac{p-1}{4})$, where the third coordinate is an integer since $p \equiv 1 \mod 4$.

□