

18.781: MIDTERM 2

APRIL 19, 2003

Instructions: To receive credit for a solution, your answer must be explained fully in complete sentences. Correct answers without proper explanation will receive no credit.

No notes, books, or calculators are allowed.

Each question is worth ten (10) points.

(1) Let p be an odd prime. Show that the equation

$$(1) \quad X^{p+1} + Y^2 \equiv 1 \pmod{p}$$

has $p - \left(\frac{-1}{p}\right)$ solutions.

We are counting pairs (x, y) such that the above equation holds. For each fixed x , the number of y 's for which the equation holds is given by

$$1 + \left(\frac{1 - x^{p+1}}{p}\right).$$

Now observe that for any x (including $x = 0$!) $x^p \equiv x \pmod{p}$, so that above expression is equal to

$$1 + \left(\frac{1 - x^2}{p}\right).$$

It follows that the total number of solutions to (1) is equal to

$$\sum_x 1 + \left(\frac{1 - x^2}{p}\right) = p + \left(\frac{-1}{p}\right) \sum_x \left(\frac{x^2 - 1}{p}\right),$$

and the last sum was shown in class (and on homework) to be -1 .

(2) For which primes p is 15 a square modulo p ?

It follows from quadratic reciprocity that

$$\left(\frac{15}{p}\right) = \left(\frac{3}{p}\right) \left(\frac{5}{p}\right) = (-1)^{(p-1)/2} \left(\frac{p}{3}\right) \left(\frac{p}{5}\right).$$

This leads us to consider two cases.

Case 1 is when $p \equiv 1 \pmod{4}$. In this case, we want $\left(\frac{p}{3}\right)$ and $\left(\frac{p}{5}\right)$ to have the same sign. Writing the squares mod 3 and 5 we find that this gives

$$p \equiv 1 \pmod{3} \text{ and } p \equiv 1 \text{ or } 4 \pmod{5}$$

or

$$p \equiv 2 \pmod{3} \text{ and } p \equiv 2 \text{ or } 3 \pmod{5}.$$

Combining all these equations with the equation $p \equiv 1 \pmod{4}$ we obtain

$$p \equiv 1, 49, 17, 53 \pmod{60}.$$

Case 2 is when $p \equiv 3 \pmod{4}$. In this case, we want $\left(\frac{p}{3}\right)$ and $\left(\frac{p}{5}\right)$ to have opposite sign. This gives

$$p \equiv 1 \pmod{3} \text{ and } p \equiv 2 \text{ or } 3 \pmod{5}$$

or

$$p \equiv 2 \pmod{3} \text{ and } p \equiv 1 \text{ or } 4 \pmod{5}.$$

Combining all these equations with the equation $p \equiv 3 \pmod{4}$ we obtain

$$p \equiv 7, 43, 11, 59 \pmod{p}.$$

Putting it all together we get

$$p \equiv 1, 7, 11, 17, 43, 49, 53, 59 \pmod{60}$$

as our final answer.

(3) Let p and q be distinct odd primes and let $\alpha \geq 1$ be an integer. How many solutions are there to the equation

$$X^q \equiv 1 \pmod{p^\alpha}?$$

Note first of all that if x is a solution of the above equation, then x must be prime to p . It follows that the derivative of $X^q - 1$ evaluated at x is non-zero. From this and Hensel's lemma we conclude that the number of solutions to the above equation mod p^α is equal to the number of solutions modulo p . We are thus reduced to the case when $\alpha = 1$.

In this case, we can choose an element γ of order $p - 1$. Then if γ^i is a solution with $i \in [1, p - 1]$, we have $\gamma^{iq} \equiv 1 \pmod{p}$ which implies that $p - 1$ divides iq . From this it follows that if $(q, p - 1) = 1$ then there is only one solution, namely 1. And if $q|p - 1$, we can write $p - 1 = qr$ for some r , and then the above shows that i must be a multiple of r . There are precisely, q such multiples in the interval $[1, p - 1]$ and hence in this case there are q solutions.

(4) (a) Evaluate the infinite simple continued fraction $\langle 1, 1, 1, \dots \rangle$.

Let ξ denote the value of $\langle 1, 1, 1, \dots \rangle$. Then

$$\xi = 1 + \frac{1}{\xi}$$

which after multiplying by ξ on both sides gives that ξ satisfies the equation

$$\xi^2 - \xi - 1 = 0.$$

The solutions to this equation are (quadratic formula)

$$\frac{1 \pm \sqrt{5}}{2}.$$

Since $\xi > 0$ we must have

$$\xi = \frac{1 + \sqrt{5}}{2}.$$

(b) Show that $k_n = h_{n-1}$ for all n (the formulas $k_n = a_n k_{n-1} + k_{n-2}$, $k_{-2} = 1$, $k_{-1} = 0$, $h_n = a_n h_{n-1} + h_{n-2}$, $h_{-2} = 0$, $h_{-1} = 1$ might be useful).

We show this by induction on n . If $n = -1$, then $k_{-1} = 0$ and $h_{-2} = 0$ by definition so that is correct. If $n = 0$, then $k_0 = k_{-2} = 1$ and $h_{-1} = 1$ by definition so that is also fine.

For general n , we can therefore assume the result holds for $n - 1$ and $n - 2$. Then since all $a_i = 1$, we have

$$k_n = k_{n-1} + k_{n-2} = h_{n-2} + h_{n-3} = h_{n-1},$$

so the result holds for n as well.

(c) Deduce that

$$\lim_{n \rightarrow \infty} \left(\xi_{n+1} + \frac{k_{n-1}}{k_n} \right) = \sqrt{5}.$$

By part (b), $\frac{k_{n-1}}{k_n} = \frac{k_{n-1}}{h_{n-1}}$ which we showed in class is equal to $1/r_{n-1}$, where we write r_{n-1} for $n - 1$ -st convergent of $\langle 1, 1, \dots \rangle$. It follows that

$$\lim_{n \rightarrow \infty} \left(\xi_{n+1} + \frac{k_{n-1}}{k_n} \right) = \lim_{n \rightarrow \infty} (\xi_{n+1} + 1/r_{n-1}) = \xi + (1/\xi).$$

Using (a) we see that this is equal to

$$\frac{1 + \sqrt{5}}{2} + \frac{-1 + \sqrt{5}}{2} = \sqrt{5}.$$

(5) Let $f(X, Y)$ be a polynomial in two variables X and Y with integer coefficients, and let p and q be distinct primes. Denote by N_p (respectively N_q) the number of solutions to the equation

$$f(X, Y) \equiv 0 \pmod{p} \quad (\text{respectively } f(X, Y) \equiv 0 \pmod{q}).$$

Show that the number of solutions to the equation

$$f(X, Y) \equiv 0 \pmod{pq}$$

is equal to $N_p \cdot N_q$.

This is exactly the same as the proof of Theorem 2.20. Note that this proof is really the statement that there is a natural bijection

(pairs of congruence classes (a, b) modulo pq)

↓

(pairs of congruence classes (a, b) modulo p) \times (pairs of congruence classes (a, b) modulo q).