

NUMBER THEORY TRACK, PROBLEM SET 3

In all of the following problems, p denotes a prime number. We think it would be a good idea if each of you would hand in your solutions to at least problems 5, 6, and problems 8 through 12, in addition to any other solutions you'd like us to take a look at.

Computations with Congruences

- (1) List all integers x in the range $1 \leq x \leq 100$ that satisfy $x \equiv 7 \pmod{17}$.
- (2) Prove that any number that is a perfect square must have one of the following for its units digit: 0, 1, 4, 5, 6, 9.
- (3) Prove that any fourth power must have one of 0, 1, 5, 6 for its units digit.
- (4) For each prime $p < 20$, create a list of all the numbers between 0 and $p - 1$ which are congruent to a square mod p .
- (5) Find a multiplicative inverse of
 - (a) $353 \pmod{400}$;
 - (b) $57 \pmod{105}$;
 - (c) $64 \pmod{105}$;
 - (d) $59 \pmod{999}$.
- (6) Find all solutions of the congruences
 - (a) $20x \equiv 4 \pmod{30}$;
 - (b) $20x \equiv 30 \pmod{4}$;
 - (c) $353x \equiv 254 \pmod{400}$;
 - (d) $57x \equiv 87 \pmod{105}$;
 - (e) $64x \equiv 83 \pmod{105}$;
 - (f) $589x \equiv 209 \pmod{817}$;
 - (g) $59x \equiv 5000 \pmod{999}$.
- (7) What is the last digit in the decimal representation of 3^{400} ? What are the last two digits?

More theorems about congruences

- (8) If $a \equiv b \pmod{m}$, show that $(a, m) = (b, m)$.
- (9) Given a and m , show that there exists x such that $(a, m) \equiv ax \pmod{m}$.
- (10) If $x^2 \equiv 1 \pmod{p}$, show that $x \equiv \pm 1 \pmod{p}$.
- (11) (*Wilson's Theorem*) This repeats and emphasizes a proof that we did in class. We'd like to calculate $(p - 1)! \pmod{p}$, since this is the product of all of the residue classes \pmod{p} . Assume that p is an odd prime.
 - (a) To start with, directly compute $2! \pmod{3}$, $3! \pmod{5}$, and $6! \pmod{7}$. Do you see a pattern?
 - (b) Write out the product for $10!$ (but don't evaluate it). Observe that there are four ways to pair up terms in the product so that the numbers in each pair are inverses of one another mod 11: the pairs are 2 and 6, 3 and 4, 5 and 9, and 7 and 8. Use this observation to conclude directly that $10! \equiv -1 \pmod{11}$.
 - (c) Use problem 10 to repeat the preceding argument in the general case. (Specifically, show that in the product for $(p - 1)!$, there are $(p - 3)/2$ pairs of inverses and two numbers which don't pair up. Which numbers don't pair up?)
- (12) Set $x = \left(\frac{p-1}{2}\right)!$. If $p \equiv 1 \pmod{4}$, use Wilson's Theorem to show that $x^2 \equiv -1 \pmod{p}$. Conclude that -1 is a square mod p if and only if $p \equiv 1 \pmod{4}$ or $p = 2$.

Binomial Coefficients

Recall that the binomial coefficient $\binom{n}{k}$, defined to be the number of size k subsets of a set of size n , is equal to $\frac{n!}{(n-k)!k!}$.

- (13) Show that $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \leq k \leq p-1$.
- (14) More generally, show that $\binom{p^\alpha}{k} \equiv 0 \pmod{p}$ for $0 < k < p^\alpha$.
- (15) Here's another proof of Fermat's Little Theorem.
- (a) Show that $0^p \equiv 0 \pmod{p}$.
 - (b) Assuming that $a^p \equiv a \pmod{p}$, prove that $(a+1)^p \equiv a+1 \pmod{p}$, and by induction conclude Fermat's Little Theorem. (Expand $(a+1)^p$ using the binomial theorem.)
- (16) If $a^p \equiv b^p \pmod{p}$, show that $a^p \equiv b^p \pmod{p^2}$.
- (17) Show that $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ for $0 \leq k \leq p-1$.
- (18) (Hard!) Show that $\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p}$.