

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

HOMEWORK 5: CONGRUENCES I

1. True or False:

- (a) $2 \equiv -5 \pmod{7}$
- (b) $55 \equiv 73 \pmod{11}$
- (c) $1111 \equiv 11 \pmod{11}$

2. For (a) and (b), compute the smallest non-negative integer in the following residue classes. For (c), reinterpret (b).

- (a) $2^{283} \pmod{17}$
- (b) $9^{2006} \pmod{100}$
- (c) What are the last (i.e. right-most) two digits of 9^{2006} ?

3. Prove or disprove: $a \equiv b \pmod{m}$ implies that $a^2 \equiv b^2 \pmod{m^2}$.

4. Is $3^{2n+5} + 2^{4n+1}$ divisible by 7 for all $n \geq 1$? Prove it.

5. Is the sum of three consecutive cubes always divisible by 9? (i.e. is $f(x) = x^3 + (x+1)^3 + (x+2)^3 \equiv 0 \pmod{9}$ for all integers $x \geq 1$)? To investigate this, make a table for $x = 1, 2, 3, 4, 5, 6, 7, 8, 9$.

6. The answer to the previous question is “Yes.” Now let’s show that the calculation we did is already enough to prove it.

(a) Show that if $x \equiv y \pmod{9}$, then $f(x) \equiv f(y) \pmod{9}$.

(b) Show that 5 and 6(a) imply that the sum of three consecutive cubes is always a multiple of 9.

7. Suppose the integer n has the base ten representation $a_m a_{m-1} \cdots a_1 a_0$, i.e.

$$n = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + 10a_1 + a_0.$$

(a) Show that $n \equiv a_0 - a_1 + a_2 - \cdots + (-1)^m a_m \pmod{11}$;

(b) Show that $11|n$ if and only if

$$a_0 - a_1 + a_2 - \cdots + (-1)^m a_m \equiv 0 \pmod{11}.$$

(c) Use (b) to check that 32323271626242003 is divisible by 11;

(d) Use (a) to check the fact the “all-ones-number” $11111 \cdots 111$ is congruent either to 1 or 0 modulo 11 depending on whether there are oddly many ones or evenly many ones.

8. Prove that if $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.

Extra Credit Problems

A. Show that if p is a fixed prime not dividing 10 (i.e. p is neither 2 nor 5), then infinitely many of the “all-ones-numbers” $1, 11, 111, 1111, \dots$ are divisible by p .

B. Characterize the odd primes p such that the congruence

$$x^2 \equiv -1 \pmod{p}$$

has a solution. Prove your answer.

C. (This is quite hard) Prove the *Bertrand Postulate* to the effect that for each integer $n \geq 1$, there is a prime in the range $n < p \leq 2n$. In other words, prove the validity of the well-known rap song (with thanks to Patrick Bolland):

Bertrand The Man

Ooh Ah Ah Ooh Ahah Ah
 Ooh Ah Ah Ooh Ahah Ah
 Bertrand said it
 and I'll say it again
 There's always a prime
 Between n and $2n$
 Ooh Ah Ah Ooh Ahah Ah
 Ooh Ah Ah Ooh Ahah Ah

D. For an integer $n \geq 1$ and a prime p in the range $n < p \leq 2n$, determine

$$v_p\left(\binom{2n}{n}\right).$$

E. Prove that for $n > 1$, the truncated harmonic series

$$h_n := 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$$

is not an integer.

Hint: One method is to consider $v_2(h_n)$. Another is to use Bertrand.

F. With h_n as above, define

$$\gamma := \lim_{n \rightarrow \infty} h_n - \log n.$$

Prove that this limit exists. We call γ the Euler or Euler-Mascheroni constant; it's a real number – find an estimate for it that you are happy with. We think that $\gamma \notin \mathbb{Q}$. No one today knows how to prove that. See what you can find out about it. Can you show that if $\gamma = a/b$ with positive integers a, b , then $b > 10$? How about $b > 100$? What's the biggest such bound for b that you could produce do you think? It is believed that no polynomial with integer coefficients could have γ as a root. Can we currently prove this even for degree 1 polynomials? Why not?