

### MATH 567 FALL 2008, NUMBER THEORY II, SOLUTIONS 3

1. Show that if  $p$  is a prime number and  $1 \leq j \leq p-1$ , then  $p$  divides the binomial coefficient  $\binom{p}{j}$ .  $p! = j!(p-j)!\binom{p}{j}$ . Moreover  $p \mid \text{LHS}$  but  $p \nmid j!(p-j)!$ .
2. Show that  $n \mid (n-1)!$  for all composite  $n > 4$ . We have  $n = ab$ ,  $1 < a < n$ . If  $a \neq b$ , then  $ab \mid (n-1)!$ . If  $a = b$ , then  $a^2 = n > 4$ ,  $a > 2$ . Thus  $a = n/a < n/2$  and  $2n = a \cdot 2a \mid (n-1)!$ .
3. Exhibit a complete residue system modulo 17 composed entirely of multiples of 3.  $3k$ ,  $0 \leq k \leq 16$ .
4. Solve  $11x \equiv 21 \pmod{105}$ .  $x \equiv 21 \pmod{105}$ .
5. Prove that  $3n^2 - 1$  can never be a perfect square.  $x^2 \equiv 0$  or  $1 \pmod{3}$ .
6. Prove that no polynomial  $f(x)$  of degree at least 1 with integral coefficients can be prime for every positive integer  $x$ . Since the degree is at least 1 we have  $|f(x)| \rightarrow \infty$  as  $x \rightarrow \infty$ . Suppose  $f(x_0) = p$  for some prime  $p$  and positive integer  $x_0$ . Then  $f(xp + x_0) \equiv f(x_0) \equiv 0 \pmod{p}$ , but for  $x$  sufficiently large  $|f(xp + x_0)| > p$ .
7. If  $2^n + 1$  is an odd prime for some integer  $n$ , prove that  $n$  is a power of 2. Suppose that  $n$  has an odd divisor  $k > 1$ . Then  $n = km$  for some  $m$ ,  $2^n + 1 = (2^m + 1)(\sum_{j=0}^{k-1} (-1)^j 2^{jm})$  and  $1 < 2^m + 1 < 2^{km} + 1 = n$ .
8. Show that if  $p$  is an odd prime, then the number of solutions (i.e., the number of ordered pairs of residues modulo  $p$ ) of the congruence  $x^2 - y^2 \equiv a \pmod{p}$  is  $p-1$  when  $a \not\equiv 0 \pmod{p}$  and  $2p-1$  when  $a \equiv 0 \pmod{p}$ . Put  $u = x+y$ ,  $v = x-y$  (1) and let  $\bar{2}$  denote the residue modulo  $p$  for which  $2\bar{2} \equiv 1 \pmod{p}$ . Then (1) holds iff  $x \equiv \bar{2}(u+v) \pmod{p}$  and  $y \equiv \bar{2}(u-v) \pmod{p}$ . Thus there is a one-to-one correspondence between the solutions of  $x^2 - y^2 \equiv a \pmod{p}$  and the solutions of  $uv \equiv a \pmod{p}$ . When  $a \not\equiv 0 \pmod{p}$ , then  $v$  is uniquely determined by  $u$  and the number of allowable choices for  $u$  is  $p-1$ . When  $a \equiv 0 \pmod{p}$ , then either  $u \equiv 0 \pmod{p}$  and  $v$  can be any residue, so there are  $p$  solutions in this case, or  $u \not\equiv 0 \pmod{p}$  and  $v \equiv 0 \pmod{p}$  in which case there are  $p-1$  solutions.