

Congruences

February 9, 2009

1. Write a single congruence that is equivalent to the pair of congruences $x \equiv 1 \pmod{4}$ and $x \equiv 2 \pmod{7}$.
2. Find the least positive integer x such that 29 divides $x^2 + 1$.
3. Let p be a prime and define $q = (p - 1)/2$. Show that if $p \equiv 3 \pmod{4}$, then $q! \equiv \pm 1 \pmod{p}$.
4. What are the last two digits in the decimal representation of 3^{5000} ?
5. Let p be prime. Evaluate $\binom{p-1}{k} \pmod{p}$.
6. Solve the congruence $15x \equiv 25 \pmod{55}$.
7. Suppose $\gcd(a, m) = 1$, and let x_1 denote a solution of $ax \equiv 1 \pmod{m}$. For $s \in \mathbb{N}$, define $x_s = 1/a - (1/a)(1 - ax_1)^s$. Prove that x_s is an integer and it is a solution of $ax \equiv 1 \pmod{m^s}$.
8. Suppose that a and m are relatively prime. This problem deals with solving $ax \equiv 1 \pmod{m^s}$. Do it first for $a = \pm 1$. Check that if m is odd and $a = \pm 2$, then $x \equiv (1 - m^s)a/4 \pmod{m^s}$ is the solution. For all other a use the previous problem to show that the solution is $x \equiv k \pmod{m^s}$ where k is the nearest integer to $-(1 - ax_1)^s/a$ and x_1 solves $ax \equiv 1 \pmod{m}$.