

Math 111, HW 4

Curtis Paul

April 29, 2007

5. Look at the equation mod 7. It becomes $2 = y^3$. But mod 7,

$$(\pm 1)^3 = \pm 1, (\pm 2)^3 = \pm 1, (\pm 3)^3 = \mp 1.$$

6. If $aa_i \equiv aa_j$, $a(a_i - a_j) \equiv 0$. $(a, n) = 1$ implies $a_i - a_j \equiv 0$, so $a_i \equiv a_j$. This means that the new representatives are independent and hence a reduced system.

7.

$$\prod a_i \equiv \prod aa_i \equiv a^{\phi(n)} \prod a_i,$$

so $a^{\phi(n)} \equiv 1$.

8. From problem 6, we see that $k, 2k, \dots, (p-1)k$ form a reduced system, so exactly one element of this list is equivalent to 1. If $k^2 \equiv 1$, $(k-1)(k+1) \equiv 0$, so $k \equiv \pm 1$.

9. Using problem 8 (not 7), the elements of $\{1, 2, \dots, p-1\}$ pair off such that $kb_k \equiv 1$, except for 1 and -1 . So the product of them all is equivalent to -1 .

10. If $n = ab$, $a \neq b$, then ab divides $(n-1)!$.

If $n = p^k$, $k > 2$, then $p(p^{k-1})$ divides $(n-1)!$.

If $n = p^2$, $p > 2$, then $p(2p)$ divides $(n-1)!$.

$3! \equiv 2 \pmod{4}$.

11. If $k^2 \equiv 1$, then $(-k)^2 \equiv 1$, so the solutions to $x^2 \equiv 1$ come in $N/2$ pairs, each pair with product -1 . The nonsolutions pair as in problem 9 to give a product of 1, so the entire product is $(-1)^{N/2}$.

13.

$$\begin{aligned} a^p &\equiv (a-1+1)^p \equiv (a-1)^p + 1, \\ (a-1)^p &\equiv (a-2+1)^p \equiv (a-2)^p + 1, \\ &\dots, \\ 2^p &\equiv (1+1)^p \equiv 1 + 1. \end{aligned}$$

Repeated substitutions yields $a^p \equiv 1 + 1 + \dots + 1 \equiv a$.

15.

$$\begin{aligned} &1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \\ &= \frac{(p-1)! + \frac{(p-1)!}{2} + \frac{(p-1)!}{3} + \dots + \frac{(p-1)!}{p-1}}{(p-1)!}. \end{aligned}$$

By Wilson's theorem, the numerator is equivalent to

$$-1(1 + 2^{-1} + 3^{-1} + \dots + (p-1)^{-1}).$$

The inverses form a reduced system, so the numerator is equivalent to

$$-1(1 + 2 + 3 + \cdots + (p - 1)) = \frac{-p(p + 1)}{2} \equiv 0.$$

$(p - 1)! \not\equiv 0$, so the numerator of

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p - 1}$$

is divisible by p .