

Math 567 Fall 2008 Number Theory I, Solutions 5

1. Prove that if $(a, m) = (a - 1, m) = 1$, then $1 + a + a^2 + \cdots + a^{\phi(m)-1} \equiv 0 \pmod{m}$, and deduce that every prime other than 2 or 5 divides infinitely many of the integers 1, 11, 111, 1111, \dots . $(1 + a + a^2 + \cdots + a^{\phi(m)-1})(a - 1) = a^{\phi(m)} - 1 \equiv 0 \pmod{m}$ by Fermat–Euler. Let $a = 10$. When $p \neq 2, 3, 5$, then $(a(a - 1), p^k) = 1$. Thus $1 + 10 + 10^2 + \cdots + 10^{\phi(p^k)-1} \equiv 0 \pmod{p^k}$ for $k = 1, 2, \dots$. When $p = 3$, $1 + 10 + 10^2 + \cdots + 10^{3t-1} \equiv 3t \equiv 0 \pmod{3}$ for $t = 1, 2, \dots$.

2. Show that every integer satisfies at least one of the following congruences; $x \equiv 0 \pmod{2}$, $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{4}$, $x \equiv 1 \pmod{6}$, $x \equiv 3 \pmod{8}$, $x \equiv 11 \pmod{12}$. Consider $x \pmod{24}$. If $x \equiv 2j$, then $x \equiv 0 \pmod{2}$. If $x \equiv 1, 5, 13, 17$, then $x \equiv 1 \pmod{4}$. If $x \equiv 3, 9, 15, 21$, then $x \equiv 0 \pmod{3}$. If $x \equiv 7, 19$, then $x \equiv 1 \pmod{6}$. If $x \equiv 11, 23$, then $x \equiv 11 \pmod{12}$. In fact the congruence $x \equiv 3 \pmod{8}$ is otiose.

3. Show that if p is an odd prime, then the congruence $x^2 \equiv 1 \pmod{p^t}$ ($t \in \mathbb{N}$) has only the two solutions $x \equiv \pm 1 \pmod{p^t}$. If $p|x - 1$ and $p|x + 1$, then $p|2 = x + 1 - (x - 1)$. Since $x^2 - 1 = (x - 1)(x + 1)$, either $p^t|x - 1$ or $p^t|x + 1$.

4. Show that the congruence $x^2 \equiv 1 \pmod{2^t}$ ($t \in \mathbb{N}$) has one solution when $t = 1$, two solutions when $t = 2$, and precisely the four solutions 1, $2^{t-1} - 1$, $2^{t-1} + 1$, -1 when $t \geq 3$. In any case x cannot be even. Thus $x \equiv 1 \pmod{2}$ is the only solution when $t = 1$ and $x \equiv 1, 3 \pmod{4}$ are the only solutions when $t = 2$. Suppose that $t > 2$ and put $x = 2y - 1$ where $0 \leq y < 2^{t-1}$. Then $4y^2 - 4y \equiv 0 \pmod{2^t}$ and this is equivalent to $y(y - 1) \equiv 0 \pmod{2^{t-2}}$ with $0 \leq y < 2^{t-1}$. Since $(y, y - 1) = 1$, either $2^{t-2}|y$ or $2^{t-2}|y - 1$. Thus the only solutions are $y = 0, 2^{t-2}, 1, 1 + 2^{t-2}$.

5. Let $n > 2$. If m is the number of solutions of the congruence $x^2 \equiv 1 \pmod{n}$, then show that $2|m$. Further let $a_1, \dots, a_{\phi(n)}$ be a system of reduced residues modulo n . Prove that $a_1 a_2 \cdots a_{\phi(n)} \equiv (-1)^{m/2} \pmod{n}$. Since $x^2 \equiv 1 \pmod{n}$ it follows that $(x, n) = 1$. If n is even, since $n > 2$, then $(n/2, n) > 1$. Thus, in any case, $x \neq n/2$. Moreover $(n - x)^2 \equiv x^2 \pmod{n}$. Thus solutions can be paired of as x and $n - x$ with $1 \leq x < n/2$. When $n > 2$, either $4|n$ or there is an odd prime p with $p|n$. Thus $\phi(n)$ is even. Consider the $\phi(n) - m$ reduced residues a which are not solutions to $x^2 \equiv 1 \pmod{n}$. Then the unique b such that $ab \equiv 1 \pmod{n}$ differs from a modulo n , and hence these reduced residues can be paired off into $(\phi(n) - m)/2$ pairs a, b such that $ab \equiv 1 \pmod{n}$. Thus it remains to consider the m residues x such that $x^2 \equiv 1 \pmod{n}$. As in the first part of the question they can be sorted into $m/2$ pairs x and $n - x$. But then $x(n - x) \equiv -x^2 \equiv -1 \pmod{n}$.

6. Show that if $n = 4^h(8k + 7)$ for some non-negative integers h and k , then $n = x^2 + y^2 + z^2$ is insoluble in integers x, y, z . Recall that $x^2 \equiv 0, 1, 4 \pmod{8}$. Suppose that $n = x^2 + y^2 + z^2$ for some x, y, z . Let 2^t be the highest power of 2 dividing (x, y, z) and put $u = x/2^t$, $v = y/2^t$, $w = z/2^t$, so that $4^t|n$ and $n/4^t = u^2 + v^2 + w^2$. One of u, v, w is odd, say w , and so $w^2 \equiv 1 \pmod{8}$. Moreover $u^2 + v^2 \equiv 0, 1, 2, 4$ or $5 \pmod{8}$. Thus $n = 4^t m$ where $m \equiv 1, 2, 3, 5$ or $6 \pmod{8}$ and so cannot be of the form $4^h(8k + 7)$.