Congruence Theorems

Thomas Belulovich

December 19, 2007

Theorems

Today, we discuss three useful theorems on congruences.

Theorem 1 (Fermat's Little Theorem)**.** Let a be an integer and p a prime integer. Then $a^p \equiv a \pmod{p}$.

Theorem 2 (Euler's Theorem)**.** Let a, n be relatively prime integers where n is positive. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Notice that Euler's theorem is a strengthening of Fermat's Little Theorem, as $\varphi(p) = p - 1$ for prime integers p.

Proof. We prove Euler's theorem. Let $k = \varphi(n)$ and let $x_1, \ldots, x_k \leq n$ be the distinct integers relatively prime to n. Then $x_1, \ldots x_k$ are distinct modulo n as well. Since $\gcd(a, n) = 1$, we have that $ax_1, \ldots ax_k$ are distinct modulo n, and each is relatively prime to n. Therefore, there exists a permutation σ of $1, 2, \ldots, k$ such that $ax_i \equiv ax_{\sigma(i)} \pmod{p}$ for each i.

So,

$$\begin{aligned} a^k \prod_i x_i &= \prod_i (ax_i) \\ &\equiv \prod_i x_i \pmod{p}, \end{aligned}$$

and therefore $a^k \equiv 1 \pmod{p}$.

□

Theorem 3 (Wilson's Theorem)**.** Let p be a prime integer. Then $(p-1)! \equiv -1 \pmod{p}$.

Proof. Assume $p \geq 3$ for otherwise the result is trivial. For nonzero residues x other than $1, -1$ modulo p, we have $x^{-1} \neq x$, and $(x^{-1})^{-1} = x$. Therefore, we can pair off multiplicative inverses, and find residues $x_1, \ldots, x_{(p-3)/2}$ such that $1, -1, x_1, x_1^{-1}, \ldots, x_{(p-3)/2}, x_{(p-3)/2}^{-1}$ form a complete set of nonzero residues modulo p. Therefore, $(p-1)! \equiv 1(-1)(x_1 x_1^{-1}) \ldots (x_{(p-3)/2} x_{(p-3)/2}^{-1}) \equiv -1 \pmod{p}$. □

Here is a secondary proof using Fermat's Little Theorem and polynomials

Proof. Consider $p(x) = x^{p-1} - 1$. By Fermat's little theorem, $p(x) = 0$ for every nonzero residue x modulo p. Therefore, $p(x) = (x-1)(x-2)\ldots(x-(p-1))$, taking coefficients mod p. So, $-1 \equiv (-1)^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. □

Examples

Exercise 1. Show that if $p \geq 5$ is a prime, then $6(p-4)! \equiv 1 \pmod{p}$.

Solution. Using Wilson's theorem, we have

$$\begin{aligned} 6(p-4)! &= -(-1)(-2)(-3)(p-4)! \\ &\equiv -(p-1)! \pmod{p} \\ &\equiv 1 \pmod{p}, \end{aligned}$$

as desired. □

Exercise 2. Define $f : \mathbb{N} \to \mathbb{Z}$ by $f(m) = 6^m + 3^m + 2^m - 1$. Find all positive integers n such that n does not divide $f(m)$ for every positive integer m.

Solution. The only such integer is $n = 1$; that $n = 1$ satisfies the condition is evident. To check that no other value for n will work, it suffices to disprove all choices of $n = p$ for some positive prime p. Suppose that $p > 3$. Then p is relatively prime to $6, 3$ and 2. Consequently,

$$\begin{aligned} 6f(p-2) = 6(6^{p-2} + 3^{p-2} + 2^{p-2} - 1) &\equiv 6^{p-1} + 2(3^{p-1}) + 3(2^{p-1}) - 6 \pmod{p} \\ &\equiv 1 + 2 + 3 - 6 \pmod{p} \qquad \text{(by Fermat's Little Theorem)} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Since $p \not| 6$, it follows that $p \mid f(p-2)$. Now, we just need to check that $p = 2$ and $p = 3$ fail. Indeed, we can see $2 \mid f(1)$ and $3 \mid f(2)$. □

Exercise 3. Find all prime numbers p and q such that pq divides the product $(5^p - 2^p)(5^q - 2^q)$.

Solution.

Lemma. Let r be a prime, and suppose that $r \mid 5^r - 2^r$. Then $r = 3$.

Proof. Clearly r is distinct from 5 and 2. The condition tells us $(5/2)^r \equiv 1 \pmod{r}$. Yet, by Fermat's little theorem, $(5/2)^{r-1} \equiv 1 \pmod{r}$. Therefore, $5 \equiv 2 \pmod{r}$ and so $r = 3$. □

WLOG, suppose $p \leq q$. Since $(5^p - 2^p)(5^q - 2^q)$ is odd, $2 \leq p \leq q$. Suppose that $p \neq 3$. Then, by the lemma, $p \mid 5^q - 2^q \implies p \mid 5^d - 2^d$, where $d = \gcd(q, p-1) = 1$, since $p - 1 < q$. Therefore, $p \mid 3 \implies p = 3$, a contradiction. Therefore, $p = 3$.

We can check that $p = 3, q = 3$ is indeed a solution. Otherwise, $q > 3$, and so $q \mid 5^3 - 2^3 = 117 = 9(13)$. Therefore, $q = 13$.

So, the solutions for (p, q) are $(3, 3), (13, 3)$, and $(3, 13)$. □

Problems

Problem 1. Find all pairs of integers (x, y) such that $x^2 = y^5 + 29$.

Problem 2. Let a, n be positive integers with $a > 1$. Show that $n \mid \varphi(a^n - 1)$.

Problem 3. Let a, m, n be integers with m and n both positive. Show that $\gcd(a^n - 1, a^m - 1) = a^{\gcd(m,n)} - 1$.

Problem 4. Let $p = 3k + 2$ be a prime dividing $a^2 + ab + b^2$ for some integers a, b. Prove that a and b are both divisible by p.

Problem 5. Let p be a prime. Show that there are infinitely many positive integers n such that p divides $2^n - n$.

Problem 6. Let $p = 4k + 1$ be a prime. Show that there is an integer x such that $x^2 \equiv -1 \pmod{p}$.

Problem 7. Show that, if n is a positive integer not divisible a square of a prime number such that n divides $2^n + 1$, then $n = 3$.