Solutions to Homework 6

Solution to problem 14. a) Let g be a primitive root modulo an odd prime p. Let g' be another primitive root modulo p. Then $g' \equiv g^k \pmod{p}$ for some k. Since

$$p-1 = \mathrm{ord}_p g' = \mathrm{ord}_p g^k = \frac{\mathrm{ord}_p g}{\gcd(\mathrm{ord}_p g, k)} = \frac{p-1}{\gcd(p-1,k)},$$

we see that $\gcd(p-1,k) = 1$. In particular, k is odd. Now $gg' = g^{1+k}$ is an even power of a primitive root, so it can not be a primitive root modulo p.

b) If $gg' \equiv 1 \pmod{p}$ then for every k we have $g^k (g')^k \equiv 1 \pmod{p}$. Thus $g^k \equiv 1 \pmod{p}$ if and only if $(g')^k \equiv 1 \pmod{p}$. In particular, g and g' have the same order modulo p. Thus g is a primitive root if and only if g' is a primitive root.

c) We know that g is its own inverse modulo p if and only if $g^2 \equiv 1 \pmod{p}$, if and only if $g \equiv \pm 1 \pmod{p}$. If $p > 3$ then -1 is not a primitive root modulo p and therefore the inverse modulo p of a primitive root is a different primitive root. Thus the primitive roots come in pairs.

Problem 1. Recall that the exponent of m is the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$ for every integer a relatively prime to m. Let m, n be integers grater than 1 such that $m|n$.

a) Suppose a is an integer relatively prime to m. Prove that there is an integer b relatively prime to n and such that $a \equiv b \pmod{m}$.

b) Let a, b be as in part a). Prove that $\mathrm{ord}_m a | \mathrm{ord}_n b$.

c) Prove that the exponent of m divides the exponent of n.

Solution. a) Let k be the product of all those prime divisors of n which do not divide m (if there are no such prime divisors, set $k = 1$). Clearly $\gcd(m,k) = 1$. An integer a is relatively prime to n if and only if it is relatively prime to both m and k. By the Chinese Remainder Theorem, there is an integer b such that $b \equiv a \pmod{m}$ and $b \equiv 1 \pmod{k}$. This implies that $\gcd(m,b) = 1 = \gcd(k,b)$, so $\gcd(n,b) = 1$.

b) Let $r = \mathrm{ord}_n b$. Then $b^r \equiv 1 \pmod{n}$. It follows that $b^r \equiv 1 \pmod{m}$. Since

$a \equiv b \pmod{m}$, we have $a^r \equiv b^r \equiv 1 \pmod{m}$. This implies that $\mathrm{ord}_m a | r$.

c) Let e be the exponent of m and f the exponenet of n. We proved that there is a such that $\mathrm{ord}_m a = e$. Let b be as in part a). Then $e|\mathrm{ord}_n b$ by part b). Since $\mathrm{ord}_n b | f$, we get $e|f$.

Problem 2. Let p be an odd prime. Consider the polynomial

$$f(x) = (x-1)(x-2)\dots(x-(p-1)) - x^{p-1} + 1.$$

a) Compute f for $p = 5$ and $p = 7$.

b) What is the degree of f?

c) What can you say about $f(i) \pmod{p}$ for $i = 1, 2, \dots, p-1$?

d) What does c) and Lagrange's Theorem tell you about the coefficients of f?

e) What is $f(0)$? Now using d) you should get a proof of Wilson's Theorem (different than the one we discussed in class).

Solution. a) When $p = 5$ we get

$$f(x) = -10x^3 + 35x^2 - 50x + 25.$$

When $p = 7$ we get

$$f(x) = -21x^5 + 175x^4 - 735x^3 + 1624x^2 - 1764x + 721.$$

b) Since

$$(x-1)(x-2)\dots(x-(p-1)) = x^{p-1} - (1+2+\dots+(p-1))x^{p-2} + \text{lower degree terms},$$

we see that the degree of f is $p-2$.

c) If $1 \le i \le p-1$, then $f(i) = -i^{p-1} + 1$ so

$$f(i) = -i^{p-1} + 1 \equiv -1 + 1 = 0 \pmod{p}$$

by Fermat's Little Theorem.

d) By b) and c) the polynomial f has degree less than $p-1$ and the congruence $f(x) \equiv 0 \pmod{p}$ has $p-1$ different modulo p solutions. By Lagrange's Theorem, this can happen only if all coefficients of f are divisible by p.

e) By d), the constant term $f(0)$ of f is divisible by p. But

$$f(0) = (-1)(-2)\dots(-p+1)+1 = 1+(-1)^{p-1}(p-1)! = 1+(p-1)!.$$

We see that p divides $1+(p-1)!$, i.e $(p-1)! \equiv -1 \pmod{p}$. Thus we preved Wilson's Theorem.

Problem 3. Let a, b be integers relatimely prime to $m > 1$. Prove that

a)

$$\mathrm{ord}_m(ab) \left| \frac{\mathrm{ord}_m(a)\mathrm{ord}_m(b)}{\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b))} \right. .$$

b) $\mathrm{ord}_m(a) | \mathrm{ord}_m(ab) \cdot \mathrm{ord}_m(b)$.

c)

$$\frac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b))} \frac{\mathrm{ord}_m(b)}{\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b))} \left| \mathrm{ord}_m(ab) \right.$$

Solution. a) Note that the number

$$N = \frac{\mathrm{ord}_m(a)\mathrm{ord}_m(b)}{\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b))} = \mathrm{ord}_m(a)\frac{\mathrm{ord}_m(b)}{\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b))} = \mathrm{ord}_m(b)\frac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b))}$$

is divisible by both $\mathrm{ord}_m(a)$ and $\mathrm{ord}_m(b)$. Thus $a^N \equiv 1 \pmod{m}$ and $b^N \equiv 1 \pmod{m}$. It follows that $(ab)^N \equiv 1 \pmod{m}$, and therefore $\mathrm{ord}_m(ab) | N$.

b) Let c be an the inverse of b modulo m. Then $\mathrm{ord}_m c = \mathrm{ord}_m b$. We have

$$a \equiv (ab)c \pmod{m} .$$

Now

$$a^{\mathrm{ord}_m(ab)\cdot\mathrm{ord}_m(b)} \equiv ((ab)c)^{\mathrm{ord}_m(ab)\cdot\mathrm{ord}_m(b)} = (ab)^{\mathrm{ord}_m(ab)\cdot\mathrm{ord}_m(b)} c^{\mathrm{ord}_m(c)\mathrm{ord}_m(ab)} \equiv 1\cdot 1 = 1 \pmod{m} .$$

This implies that $\mathrm{ord}_m(a) | \mathrm{ord}_m(ab) \cdot \mathrm{ord}_m(b)$.

c) By b) we have

$$\frac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b))} \left| \mathrm{ord}_m(ab) \frac{\mathrm{ord}_m(b)}{\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b))} \right.$$

Since the numbers $\dfrac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a),\mathrm{ord}_m(b))}$ and $\dfrac{\mathrm{ord}_m(b)}{\gcd(\mathrm{ord}_m(a),\mathrm{ord}_m(b))}$ are relatively prime, we conclude that

$$\frac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a),\mathrm{ord}_m(b))}\Bigg|\,\mathrm{ord}_m(ab).$$

Replacing the roles of a and b we show in the same way that

$$\frac{\mathrm{ord}_m(b)}{\gcd(\mathrm{ord}_m(a),\mathrm{ord}_m(b))}\Bigg|\,\mathrm{ord}_m(ab).$$

Again, since the numbers $\dfrac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a),\mathrm{ord}_m(b))}$ and $\dfrac{\mathrm{ord}_m(b)}{\gcd(\mathrm{ord}_m(a),\mathrm{ord}_m(b))}$ are relatively prime, we get

$$\frac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a),\mathrm{ord}_m(b))}\frac{\mathrm{ord}_m(b)}{\gcd(\mathrm{ord}_m(a),\mathrm{ord}_m(b))}\Bigg|\,\mathrm{ord}_m(ab).$$