MATH 115A SOLUTION SET V
FEBRUARY 17, 2005

(1) Find the orders of the integers 2, 3 and 5:
(a) modulo 17;
(b) modulo 19;
(c) modulo 23.

Solution:

(a) Euler's theorem implies that it suffices to consider exponents which are divisors of 16. Working modulo 17 gives

$$2^2 \equiv 4, \quad 2^4 \equiv 16, \quad 2^8 \equiv 1,$$
$$3^2 \equiv 9, \quad 3^4 \equiv 13, \quad 3^8 \equiv 16, \quad 3^{16} \equiv 1,$$
$$5^2 \equiv 8, \quad 5^4 \equiv 13, \quad 5^8 \equiv 16, \quad 5^{16} \equiv 1.$$

Hence it follows that 2, 3, and 5 have orders 8, 16 and 16 respectively.

(b) Consider the divisors 2, 3, 6 and 9 of 18. Working modulo 19 gives

$$2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^6 \equiv 7, \quad 2^9 \equiv 18, \quad 2^{18} \equiv 1$$
$$3^2 \equiv 9, \quad 3^3 \equiv 8, \quad 3^6 \equiv 7, \quad 3^9 \equiv 18, \quad 3^{18} \equiv 1$$
$$5^2 \equiv 6, \quad 5^3 \equiv 11, \quad 5^6 \equiv 7, \quad 5^9 \equiv 1.$$

Hence it follows that 2, 3, and 5 have orders 18, 18 and 9 respectively.

(c) Using the exponents 2, 11 and 22, and working modulo 23 gives

$$2^2 \equiv 4, \quad 2^1 1 \equiv 1$$
$$3^2 \equiv 9, \quad 3^{11} \equiv 1$$
$$5^2 \equiv 2, \quad 5^{11} \equiv 22, \quad 5^{22} \equiv 1.$$

Thus 2, 3, and 5 have orders 11, 11 and 22 respectively.

(2) Establish each of the following statements below:
(a) If a has order hk modulo n, then a^h has order k modulo n.
(b) If a has order $2k$ modulo an odd prime p, then $a^k \equiv -1 \mod p$.

Solution:

(a) Assume that a has order $hk \pmod n$, so that $a^{hk} \equiv 1 \pmod n$, but $a^m \not\equiv 1 \pmod n$ for $0 < m < hk$. Since $(a^h)^k \equiv 1 \pmod n$, it follows that the element a^h has order at most k.

Now if the order of a^h is r, with $0 < r < k$, then

$$\begin{aligned} a^{hr} &= (a^h)^r \\ &\equiv 1 \mod n, \end{aligned}$$

and this is impossible, since $hr < hk$. Hence it follows that a^h has order $k \pmod n$.

(b) Suppose that a has order $2k \pmod p$, where p is an odd prime. Then

$$a^{2k} \equiv 1 \pmod p \tag{1}$$

but $a^m \equiv 1 \pmod p$ for $0 < m < p$. Equation (1) implies that $p \mid (a^{2k} - 1)$, i.e. that $p \mid (a^k - 1)(a^k + 1)$. Therefore either $a^k \equiv 1 \pmod p$, or $a^k \equiv -1 \pmod p$. However the former possibilty cannot occur, since a has order $2k \pmod p$. It therefore follows that $a^k \equiv -1 \pmod p$, as claimed.

(3) Prove that $\phi(2^n - 1)$ is a multiple of n for any $n \geq 1$. [Hint: The integer 2 has order n modulo $2^n - 1$.]

Solution:

Plainly we have that $2^n \equiv 1 \pmod{2^n - 1}$. If $1 \leq k < n$, then $2^k - 1 < 2^n - 1$. This implies that $2^k \not\equiv 1 \pmod{2^n - 1}$, for otherwise we would have $(2^n - 1) \mid (2^k - 1)$, which is impossible. Hence it follows that the order of $2 \pmod{2^n - 1}$ is equal to n. By Euler's theorem, we have

$$2^{\phi(2^n - 1)} \equiv 1 \pmod{2^n - 1},$$

and so it follows that $n \mid \phi(2^n - 1)$.

(4) Prove the following assertions:

(a) The odd prime divisors of the integer $n^2 + 1$ are of the form $4k + 1$. [Hint: If p is an odd prime, then $n^2 \equiv -1 \mod p$ implies that $4 \mid \phi(p)$.]

(b) The odd prime divisors of the integer $n^4 + 1$ are of the form $8k + 1$.

Solution:

(a) Suppose that p is an odd prime divisor of $n^2 + 1$, so that $n^2 \equiv -1 \mod p$. This implies that $n^4 \equiv 1 \mod p$. Euler's theorem tells us that $4^{\phi(p)} \equiv 1 \mod p$, i.e. that $4^{p-1} \equiv 1 \mod p$. Hence it follows that $4 \mid (p - 1)$, and so $p = 4k + 1$ for some k.

(b) If p is an odd prime divisor of $n^4 + 1$, then $n^4 \equiv -1 \mod p$, and so $n^8 \equiv 1 \mod p$. Hence, arguing just as in part (a), it follows that $8 \mid (p - 1)$, i.e. that $p = 8k + 1$ for some k.

(5) Let r be a primitive root modulo p, where p is an odd prime. Prove the following:

(a) The congruence $r^{(p-1)/2} \equiv -1 \pmod p$ holds.

(b) If r' is any other primitive root modulo p, then rr' is not a primitive root modulo p. [Hint: From part (a), $(rr')^{(p-1)/2} \equiv 1 \pmod p$.]

(c) If the integer r' is such that $rr' \equiv 1 \pmod p$, then r' is also a primitive root modulo p.

Solution:

(a) Since r is a primitive root modulo p, $r^{p-1} \equiv 1 \pmod p$, and $p - 1$ is the smallest integer with this property. We deduce that $p \mid (r^{p-1} - 1)$, i.e. $p \mid [(r^{(p-1)/2} - 1)(r^{(p-1)/2} + 1)]$. Hence either $r^{(p-1)/2} \equiv 1 \pmod p$ or $r^{(p-1)/2} \equiv -1 \pmod p$. The first possibilty contradicts the fact that r is a primitive root modulo p. Therefore $r^{(p-1)/2} \equiv -1 \pmod p$ as claimed.

(b) If r and r' are primitive roots modulo an odd prime p, then by part (a),

$$(rr')^{(p-1)/2} \equiv r^{(p-1)/2}(r')^{(p-1)/2} \equiv -1 \cdot -1 \equiv 1 \pmod p.$$

Hence rr' has order at most $(p-1)/2$ modulo p, and so cannot be a primitive root modulo p.

(c) By Fermat's Little Theorem, we have $(r')^{p-1} \equiv 1 \pmod{p}$. If the order of r' modulo p were equal to k, with $1 \leq k < p-1$, then we would have

$$1 \equiv 1^k \equiv (rr')^k \equiv r^k(r')^k \equiv r^k \cdot 1 \equiv r^k \pmod{p},$$

which contradicts the fact that r is a primitive root modulo p. Therefore the order of r' modulo p is equal to $p-1$, and so r' is a primitive root modulo p.

(6) For any prime $p > 3$, prove that the primitive roots modulo p occur in incongruent pairs r, r', where $rr' \equiv 1 \pmod{p}$. [Hint: If r is a primitive root modulo p, consider the integer $r' = r^{p-2}$.]

Solution:

Let r be a primitive root modulo the prime $p > 3$, and set $r' = r^{p-2}$. Then $rr' = r \cdot r^{p-2} = r^{p-1} \equiv 1 \pmod{p}$. Hence, by Problem 5(c) above, we have that r' is a primitive root modulo p. Also r is not congrunet to r' modulo p, for otherwise we would have $p = 3$.

(7) Suppose that p is a prime. Use the fact that there exists a primitive root modulo p to give a different proof of Wilson's theorem. [Hint: Show that if r is a primitive root modulo p, then $(p-1)! \equiv r^{1+2+\cdots+(p-1)} \pmod{p}$.]

Solution:

If r is a primitive root modulo p, then the integers $1, 2, \ldots (p-1)$ are congruent to $r, r^2, \ldots r^{p-1}$ in some order. Hence

$$\begin{aligned}
(p-1)! &\equiv r \cdot r^2 \cdots r^{p-1} \pmod{p} \\
&\equiv r^{1+2+\cdots+(p-1)} \pmod{p} \\
&\equiv r^{p(p-1)/2} \pmod{p} \\
&\equiv (-1)^p \pmod{p} \\
&\equiv -1 \pmod{p},
\end{aligned}$$

and this proves Wilson's theorem.