2 MATH 362 Midterm 2 Time: 50 minutes

Friday November 15, 2019

1. [4] Suppose that $(a, m) = 1$ and $\operatorname{ord}_m a = t$. Prove that $a^n \equiv 1 \pmod{m}$ if and only if $t|n$.

If $n = tq$ for some $q \in \mathbb{Z}$, then

$$a^n \equiv a^{tq} \equiv (a^t)^q \equiv 1^q \equiv 1 \pmod{m}.$$

Conversely, suppose $a^n \equiv 1$ (mod m). Since t is the smallest positive integer such that $a^t \equiv 1$ (mod m), we have $n \geq t$. Dividing n by t we get

$$n = tq + r \text{ for some } q \geq 1 \text{ and } 0 \leq r < t.$$

Thus

$$1 \equiv a^n \equiv a^{tq+r} \equiv (a^t)^q a^r \equiv 1^q a^r \equiv a^r \pmod{m}.$$

Since t is the smallest positive integer such that $a^t \equiv 1$ (mod m), $a^r \equiv 1$ (mod m) with $0 \leq r < t$ is only possible if $r = 0$. Thus $n = tq$ and the result follows.

2. [4] Suppose that $\operatorname{ord}_m a = t$. Prove that $a^r \equiv a^s \pmod{m}$ <u>if and only if</u> $r \equiv s \pmod{t}$.

Suppose $a^r \equiv a^s$ (mod m). We may assume that $r \geq s$ (for otherwise we just switch r and s). Also, $(a, m) = 1$ (otherwise $\operatorname{ord}_m a$ is not defined) and so we may divide both sides of the congruence by a^s to get $a^{r-s} \equiv 1$ (mod m). By Q1, $t|(r - s)$ and thus $r \equiv s$ (mod t).

Conversely, suppose $r \equiv s$ (mod t). Then $r = kt + s$ for some integer k, and

$$a^r \equiv a^{kt+s} \equiv (a^t)^k a^s \equiv a^s (\text{mod } m)$$

because $a^t \equiv 1$ (mod m).

3. [4] Let p be an odd prime. Prove that $\operatorname{ord}_p a = 2$ if and only if $a \equiv -1 \pmod{p}$.

If $a \equiv -1 \pmod{p}$, then $a \not\equiv 1 \pmod{p}$ because p is an odd prime. Also,

$$a^2 \equiv (-1)^2 \equiv 1 \pmod{p},$$

so $\operatorname{ord}_p a = 2$.

Conversely, suppose $\operatorname{ord}_p a = 2$. Then

$$a^2 \equiv 1 \pmod{p}.$$

But p is an odd prime, so there are only two possible solutions to this congruence: $a \equiv 1$ or $a \equiv p - 1 \pmod{p}$. But the $\operatorname{ord}_p 1 = 1$, so it follows that $a \equiv p - 1 \equiv -1 \pmod{p}$.

4. [3] Let $a \in \Phi(36)$ and $\operatorname{ord}_{36} a = 6$. What is the remainder when a^{13} is divided by 36? Explain!

By a theorem, if $\operatorname{ord}_m a = t$, then $a^r \equiv a^s \pmod{m}$ iff $r \equiv s \pmod{t}$. Since $13 \equiv 1 \pmod{6}$,

$$a^{13} \equiv a^1 \pmod{36}.$$

But a is a least residue of 36, so the remainder is a.

5. [2] Euler's Criterion tells us exactly when the congruence $x^2 \equiv a \pmod{p}$ has a solution in the case where p is an odd prime. State (any form of) Euler's Criterion.

If p is an odd prime and $p \nmid a$, then $(a/p) \equiv a^{(p-1)/2} \pmod{p}$.

6. [4] Let p be an odd prime. State and prove a formula for the Legendre symbol $(-1/p)$.

If p is an odd prime, then

$$(-1/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Proof. By Euler's criterion,

$$(-1/p) \equiv (-1)^{(p-1)/2} \pmod{p}.$$

If $p \equiv 1 \pmod{4}$, then $p-1 \equiv 0 \pmod{4}$, hence $(p-1)/2$ is even and $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$.
If $p \equiv 3 \pmod{4}$, then $p-1 \equiv 2 \pmod{4}$, hence $(p-1)/2 \equiv 1 \pmod{2}$, so $(p-1)/2$ is odd and $(-1)^{(p-1)/2} \equiv -1 \pmod{p}$.
Equality follows because $(-1/p)$ is equal to either 1 or -1.

7. [3] Use Legendre symbols to determine whether the congruence $x^2 \equiv 15 \pmod{43}$ has a solution.

Determine $(15/43)$:

$$\begin{aligned} (15/43) &= (3/43)(5/43) \\ &= -(43/3)(43/5) \quad (\text{QRT; } 3 \equiv 43 \equiv 3 \pmod{4};\ 5 \equiv 1 \pmod{4} \\ &= -(1/3)(3/5) \\ &= -(5/3) \quad (\text{QRT}) \\ &= -(2/3) = -1(-1) = 1. \end{aligned}$$

Thus the congruence has a solution.

8. [6] Prove that if p and $q = 4p + 1$ are both primes, then 2 is a primitive root of q.

Because q is prime, $\phi(q) = q - 1 = 4p$. By a theorem, $\operatorname{ord}_q 2 | 4p$, so $\operatorname{ord}_p 2 \in \{1, 2, 4, p, 2p, 4p\}$. First consider $2p$. Note that $q = 4p + 1$, so $2p = \frac{q-1}{2}$. By Euler's Criterion,

$$2^{2p} \equiv 2^{(q-1)/2} \equiv (2/q) \pmod{q}.$$

We know p is odd; say $p = 2k + 1$ for some k. Then $4p = 8k + 4$, that is, $4p \equiv 4 \pmod{8}$ and so $q \equiv 4 + 1 \equiv 5 \pmod{8}$. Hence $(2/q) = -1$ and so

$$2^{2p} \equiv (2/q) \equiv -1 \pmod{q}.$$

Therefore $\operatorname{ord}_q 2 \neq 2p$.

Suppose $d|2p$. Then $\operatorname{ord}_p 2 \neq d$, otherwise Q1 would imply that $2^{2p} \equiv 1 \pmod{q}$ which is not the case. Therefore $\operatorname{ord}_q 2 \notin \{1, 2, p\}$.

Suppose $\operatorname{ord}_q 2 = 4$. Then

$$1 \equiv 2^4 \equiv 16 \pmod{q}$$

and so $q|15$. Since q is a prime of the form $4p + 1$, the only possibility is $q = 5$. But then $p = 1$, which is not the case as p is prime. Hence $\operatorname{ord}_q 2 \neq 4$.

Therefore $\operatorname{ord}_q 2 = 4p$ and 2 is a primitive root of q.

9. [4] Find the period and the length of the non-periodical part of the expansion of 15/756 in base 14.

First write 15/756 in lowest form: $15/756 = 5/252$.

Factorize 252: $252 = 2^2 7^1 3^2 = 28 \cdot 9$, where $(9, 14) = 1$.

The period of the expansion is $\operatorname{ord}_9 14 = \operatorname{ord}_9 5$. Since $\phi(9) = 6$, we determine 5^t, where $t = 2, 3, 6$:

$$\begin{aligned} 5^2 &\equiv 25 \equiv 7 \pmod{9} \\ 5^3 &\equiv 35 \equiv -1 \pmod{9} \\ 5^6 &\equiv 1 \pmod{9}. \end{aligned}$$

So the period of the expansion is 6.

The length of the nonperiodical part is $\max\{2, 1\} = 2$.