

Math 104A, Number Theory, Fall 2002.
Summary of Lecture 26.

What's on the Final Exam? 5 standard calculation questions, 2 proof questions and a surprise.

What's a standard calculation question? Could be finding a prime factorization, computing extended Euclidean algorithm, solving linear diophantine equations, linear congruences, Chinese remainder theorem, polynomial congruences, computation of powers modulo m , computation of Euler's totient function, computation of the number of roots of $x^r \equiv \pm 1 \pmod{p}$.

Last time: Corollary 2 to Lagrange's Theorem. Let p be prime and suppose $d > 0$. Then $x^d - 1$ has $(d, p - 1)$ distinct roots modulo p . (These may not be simple.)

Example. If p is an odd prime then $x^2 \equiv 1 \pmod{p}$ has precisely two solutions, $x \equiv \pm 1 \pmod{p}$. You can see this from Corollary 2 by setting $d = 2$. Since p is an odd prime, $(d, p - 1) = 2$ and there are 2 solutions. You can also see it as follows:

$$x^2 \equiv 1 \pmod{p} \iff p|(x-1)(x+1) \iff p|(x-1) \text{ or } p|(x+1) \iff x \equiv \pm 1 \pmod{p}.$$

Corollary 3. Let p be an odd prime and suppose $d > 0$. Then $x^d + 1$ has $(2d, p - 1) - (d, p - 1)$ distinct roots modulo p . (These may not be simple.)

Proof.

$$x^p + 1 \equiv 0 \pmod{p} \iff x^p \equiv -1 \pmod{p} \iff x^{2d} \equiv 1 \pmod{p} \text{ and } x^d \not\equiv 1 \pmod{p}.$$

Since the number of values x modulo p with $x^{2d} \equiv 1 \pmod{p}$ is $(2d, p - 1)$ and the number of values x modulo p with $x^d \equiv 1 \pmod{p}$ is $(d, p - 1)$, we get the result.

We consider $n = pq$, with p and q distinct odd. Our aim is to show that if you know e and d with $ed \equiv 1 \pmod{\phi(n)}$ then you can factorize n . We introduced the algorithm to do this which is given on the bottom half of page 139, and we almost completed the proof of Theorem 5.3.7.