Final Review

Tim Smits

1. Let a, n be integers with $n > 1$. Suppose that $a^{n-1} \equiv 1 \bmod n$ and $a^d \not\equiv 1 \bmod n$ for every proper divisor d of $n-1$. Prove that n is prime.

2. (a) Let a, n be positive integers with $(a, n) = 1$. Suppose that $(k, \varphi(n)) = 1$. Prove that the equation $x^k \equiv a \bmod n$ has a unique solution.

   (b) Find the solution to $x^7 \equiv 21 \bmod 23$.

3. Let p be an odd prime, and suppose $p = a^2 + b^2$ where a is odd. Prove that a is a square mod p.

4. Suppose that $n = 4^e(8k + 7)$ for some $e, k \geq 0$. Prove that n is not a sum of three squares. (It's actually true that any integer not of this form *is* a sum of three squares, but it's very hard to prove!)

5. (a) Let a, n be positive integers with $a \geq 2$. Prove that $n \mid \varphi(a^n - 1)$.

   (b) Prove that if $p \mid \varphi(n)$ and $p \nmid n$ then there is a prime factor q of n with $q \equiv 1 \bmod p$.

   (c) Let p be a prime. Prove there are infinitely many primes $q \equiv 1 \bmod p$.

Hints

1. Case on the number of prime factors of n.

2a. Bezout's lemma.

2b. Find a generator mod 23.

3. Use Jacobi symbols.

4. First handle the case that $e = 0$.

5a. What is $\mathrm{ord}_{a^n-1}(a)$?

5b. Compute $\varphi(n)$ in terms of a prime factorization of n.

5c. Suppose there are finitely many primes $p_1, \ldots, p_k$ with $p_i \equiv 1 \bmod p$. Set $a = pp_1 \cdots p_k$. Choose a suitable exponent to apply parts (a) and (b).

Solutions

1. Suppose that n is composite. First, suppose that n has at least two distinct prime factors. Then we may write $n = k\ell$ for some $k\ell$ with $(k, \ell) = 1$. We have $\varphi(n) = \varphi(k)\varphi(\ell)$, and by Euler's theorem, $a^{\varphi(n)} \equiv 1 \bmod n$. The assumptions in the problem say that $\mathrm{ord}_n(a) = n-1$, so this means $n - 1 \mid \varphi(n) = \varphi(k)\varphi(\ell)$. Since $\varphi(k) \leq k - 1$ and $\varphi(\ell) \leq \ell - 1$, we see that $\varphi(n) \leq (k-1)(\ell-1) = n - (k + \ell - 1) < n - 1$. This is a contradiction. This leaves only the case where $n = p^e$ for some prime p. In this case, $\varphi(n) = \varphi(p^e) = p^{e-1}(p-1)$ and this is clearly not divisible by $p^e - 1$, which is also a contradiction. Therefore, n is prime.

2. (a) Suppose that $x^k \equiv a \bmod n$ and $y^k \equiv a \bmod n$, so that $x^k \equiv y^k \bmod n$. Since $(a, n) = 1$, this means that $(x, n) = 1$ and $(y, n) = 1$. Thus, $(x/y)^k \equiv 1 \bmod n$. By Bezout's lemma, there are integers a, b with $ak + b\varphi(n) = 1$. Since $(x/y)^{\varphi(n)} \equiv 1 \bmod n$ by Euler's theorem, we have $(x/y) = (x/y)^{ak+b\varphi(n)} = ((x/y)^k)^a \cdot ((x/y)^{\varphi(n)})^b \equiv 1^a \cdot 1^b \equiv 1 \bmod n$, so that $x \equiv y \bmod n$ as desired.

   (b) We have $22 = 2 \cdot 11$. Note that 5 is a generator mod 23: we must have $\mathrm{ord}_{23}(5) \mid 22$, so it's either $2, 11$, or 22. We compute that $5^2 \equiv 2 \bmod 23$ and $5^{11} \equiv -1 \bmod 23$, so the only remaining possibility is that $\mathrm{ord}_{23}(5) = 22$. Note that $21 \equiv -2 \bmod 23$, so $21 \equiv 5^{13} \bmod 23$. Since 5 is a generator, we may write $x \equiv 5^k \bmod 23$ for some k. We wish to solve $5^{7k} \equiv 21 \bmod 23$. Taking a discrete log, we have $7k \equiv \log_5(21) \bmod 22$, so $7k \equiv 13 \bmod 22$. One can check that $\frac{1}{7} \equiv 19 \bmod 22$, so $k \equiv 13 \cdot 19 \equiv 5 \bmod 22$. Thus, $x \equiv 5^5 \equiv 20 \bmod 23$ is the solution.

3. This is equivalent to showing that $\left(\frac{a}{p}\right) = 1$. Write $a = p_1^{e_1} \cdots p_k^{e_k}$. Since p is a sum of two squares, we must have $p \equiv 1 \bmod 4$. By Jacobi reciprocity and properties of the Jacobi symbol, we have $\left(\frac{a}{p}\right) = \left(\frac{p}{p_1}\right)^{e_1} \cdots \left(\frac{p}{p_k}\right)^{e_k}$. Since $p_i \mid a$, we have $p \equiv b^2 \bmod p_i$, so that $\left(\frac{p}{p_i}\right) = 1$ for each i. Thus, $\left(\frac{a}{p}\right) = 1$.

4. First, suppose that $e = 0$. Then $n = 8k + 7$, so $n \equiv 7 \bmod 8$. If $n = x^2 + y^2 + z^2$, then $x^2 + y^2 + z^2 \equiv 7 \bmod 8$. The squares mod 8 are $0, 1, 4 \bmod 8$. Since n is odd, an odd number of these three squares must equal $1 \bmod 8$. Clearly all three of them can't, which means exactly one of them is. This means the remaining two squares sum to $6 \bmod 8$, and it's easy to see that this is impossible. Now, suppose that $e \geq 1$ and $n = x^2 + y^2 + z^2$. Then $x^2 + y^2 + z^2 \equiv 0 \bmod 4$. The squares mod 4 are $0, 1 \bmod 4$, so the only way this is possible is if $x^2, y^2, z^2 \equiv 0 \bmod 4$, i.e. x, y, z are even. Then $n/4 = (x/2)^2 + (y/2)^2 + (z/2)^2$. Repeating this, $n/4^e = (x/2^e)^2 + (y/2^e)^2 + (z/2^e)^2$, a contradiction to the $e = 0$ case. Thus, no n of such a form is a sum of three squares.

5. (a) Clearly, $(a, a^n - 1) = 1$. By Euler's theorem, we have $a^{\varphi(a^n-1)} \equiv 1 \bmod a^n - 1$. Note that $a^n - 1 \equiv 0 \bmod a^n - 1$, so $a^n \equiv 1 \bmod a^n - 1$. We now show that $\mathrm{ord}_{a^n-1}(a) = n$. Suppose otherwise, that $\mathrm{ord}_{a^n-1}(a) = d$ for some $d \mid n$. Then $a^d \equiv 1 \bmod a^n - 1$ says $a^n - 1 \mid a^d - 1$, which is impossible since $d < n$. Therefore, $\mathrm{ord}_{a^n-1}(a) = n$, so that $n \mid \varphi(a^n - 1)$ as desired.

   (b) Let $n = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of n. Then $\varphi(n) = p_1^{e_1-1} \cdots p_k^{e_k-1}(p_1 - 1) \cdots (p_k - 1)$. Since $p \nmid n$, then $p \neq p_i$ for any i. Since $p \mid \varphi(n)$, this means that $p \mid (p_i - 1)$ for some i, i.e. $p_i \equiv 1 \bmod p$ for some i.

   (c) Suppose there are finitely many primes $p_1, \ldots, p_k$ with $p_i \equiv 1 \bmod p$. Set $a = pp_1 \cdots p_k$. Then by part (a), we have $p \mid \varphi(a^p - 1)$. Since $a^p - 1 = (pp_1 \cdots p_k)^p - 1$, then $p \nmid a^p - 1$. By part (b), there is a prime factor q of $a^p - 1$ with $q \equiv 1 \bmod p$. However, note that $a^p - 1 \equiv -1 \bmod p_i$, so $a^p - 1$ is not divisible by any of the primes that are $1 \bmod p$. This is a contradiction. Therefore, there are infinitely many primes $q \equiv 1 \bmod p$.