
Math 242: Homework 4

John Peca-Medlin

April 26, 2006

Chapter 4:

4. Let p be a prime of the form $4t + 1$ and a a primitive root modulo p . If $-1 \equiv a^n \pmod{p}$, then we have $a^{2n} \equiv 1 \pmod{p}$, and thus by definition $\phi(p) = p - 1 \mid 2n$ since $p - 1 = 4t$ is the minimal positive integer with this property for the primitive root a . We see $p - 1 \mid 2n$ iff $\frac{1}{2}(p - 1) = 2t \mid n$. If n is odd, then we have $2 \mid n$, a contradiction. Thus, it is necessary that n be even. Then $(-1)^n = 1$ and so we have $(-a)^n \equiv 1 \pmod{p}$ iff $a^n \equiv 1 \pmod{p}$. Thus, $(-a)^{p-1} \equiv 1 \pmod{p}$ iff $a^{p-1} \equiv 1 \pmod{p} \implies a$ is a primitive root modulo p iff $-a$ is a primitive root modulo p , as desired.

8. (\implies) Let a be a primitive root modulo p . Then by definition, $p - 1$ is the least positive integer such that $a^{p-1} \equiv 1 \pmod{p}$. Since $(p - 1)/q < p - 1$ for all prime divisors q of $p - 1$, we then have $a^{(p-1)/q} \not\equiv 1 \pmod{p}$.

(\impliedby) Assume $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p - 1$. By Fermat's Little Theorem, for $p \nmid a$, we have $a^{p-1} \equiv 1 \pmod{p}$. We just need to prove the minimality of $p - 1$ for this property. By Proposition 4.2.1, we have a is an n^{th} power residue modulo p iff $a^{\phi(p)/d} \equiv 1 \pmod{p}$ with $d = (n, \phi(p))$. Thus, we see if a is not a generator, then its order n divides $p - 1$, hence n divides $(p - 1)/q$ for some prime divisor q of $p - 1$. It follows that $a^{(p-1)/q} \equiv 1 \pmod{p}$, a contradiction. Therefore, a must be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and thus a primitive root modulo p .

20. The result is straightforward for $p = 2$, so assume p to be an odd prime. For d a divisor of $p - 1$, let $d' = (p - 1)/d$ and a a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ (which exists since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic). So every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a multiple of a , and $a^{dd'} = a^{p-1} \equiv 1 \pmod{p}$ and $p - 1$ is the smallest positive integer such that this holds. Let $\varphi_d : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ be defined by the action $a \mapsto a^d$. It is easy to see that φ_d is indeed a group homomorphism ($\varphi_d(\alpha\beta) = (\alpha\beta)^d = \alpha^d\beta^d = \varphi_d(\alpha)\varphi_d(\beta)$), and thus that $\text{Im } \varphi_d$, which consists of the d^{th} powers, is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ (it preserves the identity, inverses, and associativity, and we see if $\alpha, \beta \in \text{Im } \varphi_d$, then $\alpha\beta \in \text{Im } \varphi_d$ simply by the property of φ_d being a homomorphism already mentioned). To see that $\text{Im } \varphi_d$ is of order d' , note that by the minimality of $p - 1$ for the relation $a^{p-1} \equiv 1 \pmod{p}$ to hold, we have d' is the minimal positive integer such that $(a^d)^{d'} \equiv 1 \pmod{p}$, otherwise a could not be a generator as we assumed. Thus we have by definition that the order of our resulting subgroup is $d' = (p - 1)/d$.

For $p = 11$, $d = 5$, we see $(p - 1)/d = 10/5 = 2$, which says we will have a subgroup of order 2. We see this is true since $1^5 \equiv 3^5 \equiv 4^5 \equiv 5^5 \equiv 9^5 \equiv 1 \pmod{11}$ and $2^5 \equiv 6^5 \equiv 7^5 \equiv 8^5 \equiv 10^5 \equiv 1 \pmod{11}$, and our resulting subgroup is just $\{1, 10\}$. By the last homework, we already knew there were only 2 solutions to the equation $x^{(11-1)/5} = x^2 \equiv 1 \pmod{11}$, which were 1 and $p - 1$, our resulting subgroup.

For $p = 17$, $d = 4$, we see $(p - 1)/d = 16/4 = 4$, so we will have a subgroup of order 4. Indeed, since we have $1^4 \equiv 4^4 \equiv 13^4 \equiv 16^4 \equiv 1 \pmod{17}$, $6^4 \equiv 7^4 \equiv 10^4 \equiv 11^4 \equiv 4 \pmod{17}$, $3^4 \equiv 5^4 \equiv 12^4 \equiv 14^4 \equiv 13 \pmod{17}$, and $2^4 \equiv 8^4 \equiv 9^4 \equiv 15^4 \equiv 16 \pmod{17}$, our resulting subgroup is $\{1, 4, 13, 16\}$.

For $p = 19$, $d = 6$, we see $(p - 1)/d = 18/6 = 3$, so we will have a subgroup of order 3. This is true since we have $1^6 \equiv 7^6 \equiv 8^6 \equiv 11^6 \equiv 12^6 \equiv 18^6 \equiv 1 \pmod{19}$, $2^6 \equiv 3^6 \equiv 5^6 \equiv 14^6 \equiv 16^6 \equiv 17^6 \equiv 7 \pmod{19}$, and $4^6 \equiv 6^6 \equiv 9^6 \equiv 10^6 \equiv 13^6 \equiv 15^6 \equiv 11 \pmod{19}$, giving us a subgroup $\{1, 7, 11\}$, which is of order 3.

Chapter 5:

1. Gauss' Lemma states $(a \mid p) = (-1)^\mu$, with μ being the number of negative least residues. Thus, for $p = 7$ and $a = 5$, we see $(p - 1)/2 = 3$ and $1 \cdot 5, 2 \cdot 5, 3 \cdot 5$ are congruent to $-2, 3$, and 1 modulo 7. So $\mu = 1$, and thus $(5 \mid 7) = (-1)^\mu = (-1)^1 = -1$.

For $p = 11$ and $a = 3$, we see $(p - 1)/2 = 5$ and $1 \cdot 3, 2 \cdot 3, 3 \cdot 3, 4 \cdot 3, 5 \cdot 3$ are congruent to $1, -5, -2, 1,$ and 4 modulo 11 . So $\mu = 2$, and we have $(3 | 11) = (-1)^\mu = (-1)^2 = 1$. Indeed, $5^2 \equiv 6^2 \equiv 3 \pmod{11}$.

For $p = 13$ and $a = 6$, we see $(p - 1)/2 = 6$ and $1 \cdot 6, 2 \cdot 6, 3 \cdot 6, 4 \cdot 6, 5 \cdot 6, 6 \cdot 6$ are congruent to $6, -1, 5, -2, 4,$ and -3 modulo 13 . So $\mu = 3$, and we have $(6 | 13) = (-1)^\mu = (-1)^3 = -1$.

And last, for p an odd prime and $a = -1$, we see $1(-1), 2(-1), 3(-1), \dots, (p - 1)/2(-1)$ would form a total of $(p - 1)/2$ negative least residues (since each would be a negative least residue). So $\mu = (p - 1)/2$, and we have $(-1 | p) = (-1)^\mu = (-1)^{(p-1)/2}$. Thus, $(-1 | p) = 1$ iff $p \equiv 1 \pmod{4}$ and $(-1 | p) = -1$ iff $p \equiv 3 \pmod{4}$.

6. Let p be an odd prime. We need to count the pairs (x, y) such that the equation $x^2 - y^2 \equiv a \pmod{p}$ holds. First, rewrite the equation $x^2 \equiv y^2 + a \pmod{p}$. We see if $y^2 + a$ is a nonresidue, then there are 0 solutions since there would be no x for which the equation could hold. If $y^2 + a$ is a residue, then there are 2 solutions since if $\alpha^2 \equiv y^2 + a \pmod{p}$ then we also have $(-\alpha)^2 \equiv y^2 + a \pmod{p}$ and $\alpha \neq -\alpha$ since p is odd, and also there cannot be another element that is a square root modulo p of $y^2 + a$ since by Problem 20 above the action $a \mapsto a^2$ would form a subgroup of order $(p - 1)/2$ and thus there exist at most 2 square roots per element in the resulting subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. Last, if the equation is divisible by p , then there is only one solution, namely $x = 0$. Thus, for each fixed y , the number of x 's for which the equation holds is given by $1 + ((y^2 + a) | p)$. So summing over all elements in $\mathbb{Z}/p\mathbb{Z}$, we see then that the total number of solutions are $\sum_{y=0}^{p-1} (1 + ((y^2 + a) | p))$, as desired.

7. Using the hint, let $u = x + y$ and $v = x - y$, so the equation $x^2 - y^2 \equiv a \pmod{p}$ becomes $uv \equiv a \pmod{p}$. If $p \nmid a$, we have $p \nmid uv$. Since we know $p \nmid uv$ for $uv \in \{1, 2, \dots, p - 1\}$, we see there are only $p - 1$ distinct choices for uv (with respect to the least residues, there are $(p - 1)/2$ choices for which $u = x + y < x - y = v$ and $(p - 1)/2$ choices for which $u = x + y > x - y = v$), and thus $p - 1$ solutions to the equation if $p \nmid a$.

If $p | a$, then $p | uv$. Since p is prime, then either $p | u$ or $p | v$. Since 0 is the only option such that p could divide either u or v , we see there are p choices for v if $u = 0$ (including $v = 0$), i.e. $x = -y$, and $p - 1$ choices for u if $v = 0$ (excluding $u = 0$), i.e. $x = y$. So in total, there are $2p - 1$ solutions if $p | a$, as we wanted to show.

8. Note: $\sum_{y=0}^{p-1} (1 + ((y^2 + a) | p)) = \sum_{y=0}^{p-1} 1 + \sum_{y=0}^{p-1} ((y^2 + a) | p) = p + \sum_{y=0}^{p-1} ((y^2 + a) | p)$. If $p \nmid a$, by the previous problem there are $p - 1$ total solutions to the equation $x^2 - y^2 \equiv a \pmod{p}$. Thus, $\sum_{y=0}^{p-1} ((y^2 + a) | p) = \sum_{y=0}^{p-1} (1 + ((y^2 + a) | p)) - p = (p - 1) - p = -1$.

If $p | a$, then by the previous problem there are $2p - 1$ total solutions to our favorite equation. Thus, $\sum_{y=0}^{p-1} ((y^2 + a) | p) = \sum_{y=0}^{p-1} (1 + ((y^2 + a) | p)) - p = (2p - 1) - p = p - 1$, as we wanted to show.

24. For $p \equiv 1 \pmod{4}$, let m be such that $p = 4m + 1$. Using Wilson's Theorem, we see $n = (2m)!$ is a square root of -1 modulo p . Thus, working inside $\mathbb{Z}[i]$, we see $p | n^2 + 1 = (n - i)(n + i)$ and hence p is not irreducible since $p \nmid n - i$ and $p \nmid n + i$. So we know there exist $a, b, c, d \in \mathbb{Z}$ such that $p = (a + bi)(c + di)$. Since $\mathbb{Z}[i]$ is a Euclidean domain with Euclidean norm $|\cdot|$, we see $|p|^2 = p^2 = |(a + bi)(c + di)|^2 = |a + bi|^2 |c + di|^2 = (a^2 + b^2)(c^2 + d^2)$. Since we see neither factor of p has norm 1, then we must have $p = a^2 + b^2 = c^2 + d^2$, and so we are done.

29. Note for $\{1, 2, \dots, p - 1\}$ there are a total of $p - 2$ consecutive pairings, thus we will have $(RR) + (NR) + (RN) + (NN) = p - 2$ and so $(RR) + (NR) = p - 2 - ((RN) + (NN))$ and $(RR) + (RN) = p - 2 - ((NR) + (NN))$. Also, using the results from Problem 1 for Chapter 5 above, we see using the property $(ab | p) = (a | p)(b | p)$ from Proposition 5.1.2, gives us if $p \equiv 1 \pmod{4}$, then $(-a | p) = (-1 | p)(a | p) = (a | p)$ and thus $(a | p) = 1$ iff $(-a | p) = 1$. By Corollary 1 in this chapter, we see there are the same number of residues as nonresidues, that is both are $(p - 1)/2$.

Thus, so for the case $p \equiv 1 \pmod{4}$, we see $(RN) + (NR) + (NN) + [(RR) + 1] = p - 2$ and so $(RN) = (NR) = (NN) = (p - 1)/4$ and $(RR) = (p - 1)/4 - 1$. So we have $(RR) + (RN) = (RR) + (NR) = 2\frac{p-1}{4} - 1 = \frac{p-3}{2}$ and $(NR) + (NN) = (RN) + (NN) = p - 2 - \frac{p-3}{4} = \frac{p-1}{2}$.

And last, for the case $p \equiv 3 \pmod{4}$, we see $(RR) + (NR) + (NN) + [(RN) - 1] = p - 2$ and so $(RR) = (NR) = (NN) = \frac{p-3}{4}$ and $(RN) = \frac{p-3}{4} + 1 = \frac{p+1}{4}$. So we have $(NR) + (NN) = (RR) + (NR) = 2\frac{p-3}{4} = \frac{p-3}{2}$ and $(RN) + (NN) = (RR) + (RN) = p - 2 - \frac{p-3}{2} = \frac{p-1}{2}$.