Solutions to Homework 8

Tim Smits

March 12, 2022

1.

(a) Solve the equation $4^x \equiv 25 \bmod 59$ *(Hint: 2 is a generator mod 59.)*

(b) Find all solutions to $f(x) \equiv 0 \bmod 6125$ where $f(x) = x^6 - 2x^5 - 35$. (Note: $6125 = 5^3 \cdot 7^2$).

Solution:

(a) Note that $5 \equiv 64 \equiv 2^6 \bmod 59$, and so we wish to solve the equation $4^x \equiv 2^{12} \bmod 59$, i.e. $2^{2x} \equiv 2^{12} \bmod 59$. Since exponentiation only matters mod 58, we want to solve $2x \equiv 12 \bmod 58$. Dividing through by 2 yields $x \equiv 6 \bmod 29$, so $x \equiv 6, 35 \bmod 58$ are the solutions to $2x \equiv 12 \bmod 58$, and therefore the solutions to $4^x \equiv 25 \bmod 59$. Explicitly, this says our solutions are $4^6, 4^{35} \bmod 59$.

(b) By the Chinese remainder theorem, solving $f(x) \equiv 0 \bmod 6125$ is equivalent to solving the system of equations $f(x) \equiv 0 \bmod 5^3$ and $f(x) \equiv 0 \bmod 7^2$.

Let's start with the first congruence. If r is a solution to $f(x) \equiv 0 \bmod 5^3$, then $f(r) \equiv 0 \bmod 5^3$ and so in particular, we must have $f(r) \equiv 0 \bmod 5$. The solutions to $f(x) \equiv 0 \bmod 5$ are $x \equiv 0, 2$. We have $f'(x) = 6x^5 - 10x^4$ and $f'(0) \equiv 0 \bmod 5$, $f'(2) = 32 \not\equiv 0 \bmod 5$. By Hensel's lemma, the latter root lifts to a root mod 5^k for any $k \geq 1$, and therefore there is a single solution to $f(x) \equiv 0 \bmod 5^3$, given by the lift of the root 2. To figure this out, first let's lift it to a root mod 25. Set $c_1 = 2$ and $c_2 = 2 + 5t_2$. Then we wish to solve for t_2 that makes $f(c_2) \equiv 0 \bmod 25$. We have $f(c_2) \equiv f(2) + f'(2) \cdot 5t_2 \bmod 25$. We have $f(2) = -35$, and therefore dividing by 5 we wish to solve $-7 + 32t_2 \equiv 0 \bmod 5$, i.e. $3 + 2t_2 \equiv 0 \bmod 5$. This yields $t_2 \equiv 1 \bmod 5$, so we may take $c_2 = 2 + 5 \cdot 1 = 7 \bmod 25$. Now we want to lift again, but we actually don't have to: $f(7) = 84000$ which is divisible by 125, and therefore $x \equiv 7 \bmod 125$. Note that 0 doesn't lift up: $f(5t_2) \equiv 0 \bmod 25$ if and only if $f(0) + f'(0) \cdot 5t_2 \equiv 0 \bmod 25$, which is the same as saying that $f(0) \equiv 0 \bmod 25$, which is clearly false. Therefore, $x \equiv 7 \bmod 125$ is the unique solution to $f(x) \equiv 0 \bmod 125$.

Next, we do this procedure to find the roots of $f(x) \bmod 49$. The solutions to $f(x) \equiv 0 \bmod 7$ are $x \equiv 0, 2 \bmod 7$ and again we have $f'(0) \equiv 0 \bmod 7$ and $f'(2) = 32 \not\equiv 0 \bmod 7$, so there is a single root mod 49. Set $c_1 = 2$ and $c_2 = 2 + 7t_2$. We wish to solve for t_2 that makes $f(c_2) \equiv 0 \bmod 49$. We have $f(c_2) \equiv f(2) + f'(2) \cdot 7t_2 \bmod 125$. Plugging in, and dividing by 7, we wish to solve $-5 + 32t_2 \equiv 0 \bmod 7$, i.e. $2 + 4t_2 \equiv 0 \bmod 7$. We see that $t_2 \equiv 3 \bmod 7$ solves this equation, and so we can take $c_2 = 2 + 7 \cdot 3 = 23 \bmod 49$. Similarly, 0 doesn't lift up and so $x \equiv 23 \bmod 49$ is the unique solution to $f(x) \equiv 0 \bmod 49$.

Therefore, by the Chinese remainder theorem, there is a single solution to $f(x) \equiv 0 \bmod 6125$ given by $x \equiv 7 \bmod 125$ and $x \equiv 23 \bmod 49$. Solving this yields $x \equiv 3257 \bmod 6125$.

2. Prove that for any $k \geq 1$, there are exactly $p-1$ distinct elements of $\mathbb{Z}/p^k\mathbb{Z}$ that satisfy $x^{p-1} = [1]$.

Solution: Consider the polynomial $f(x) = x^{p-1} - 1 \in \mathbb{Z}[x]$. By Fermat's little theorem, we have $f(c_i) \equiv 0 \bmod p$ for $c_i = i$ with $1 \leq i \leq p-1$, and $f'(c_i) = (p-1)c_i^{p-2} \equiv -c_i^{p-2} \not\equiv 0 \bmod p$. These are all the roots of $f(x)$ mod p, because a degree $p-1$ polynomial cannot have more than $p-1$ roots mod p. By Hensel's lemma, each root lifts up to a root of $f(x)$ mod p^k for any $k \geq 1$. This says $f(x)$ has at least $p-1$ roots mod p^k. On the other hand, if r is a root of $f(x)$ mod p^k then $f(r) \equiv 0 \bmod p^k$, so certainly $f(r) \equiv 0 \bmod p$. In particular, $r \equiv c_i \bmod p$ for some choice of i and therefore by the uniqueness of Hensel's lemma, r must be some lift of c_i. This says there are at most $p-1$ roots, so there are exactly $p-1$ roots of $f(x)$ mod p^k. Translating into a statement about $\mathbb{Z}/p^k\mathbb{Z}$, this says there are exactly $p-1$ solutions to $x^{p-1} = [1]$ as desired.

3.

(a) Let p be an odd prime, and let a, k be integers with $p \nmid a$. Prove that $x^k \equiv a \bmod p$ is solvable if and only if $a^{\frac{p-1}{d}} \equiv 1 \bmod p$, where $d = \gcd(k, p-1)$. *(Hint: work in terms of a generator g.)*

(b) Find all solutions to $x^5 \equiv 6 \bmod 101$.

Solution:

(a) Let g be a generator mod p. Any solution to $x^k \equiv a \bmod p$ may be written as $x \equiv g^r \bmod p$ for some r, and we may write $a \equiv g^s \bmod p$ for some s. Therefore, solving the equation $x^k \equiv a \bmod p$ is the same as solving the equation $g^{rk} \equiv g^s \bmod p$ for r. Since exponentiation only matters mod $p-1$, this equation is solvable if and only if $rk \equiv s \bmod p-1$. From homework 3, we know such an equation is solvable if and only if $d \mid s$, where $d = \gcd(k, p-1)$. Now, we will prove $d \mid s$ if and only if $a^{\frac{p-1}{d}} \equiv 1 \bmod p$, and then we'll be done. Suppose that $d \mid s$. Then $a^{\frac{p-1}{d}} \equiv (g^s)^{\frac{p-1}{d}} \equiv (g^{p-1})^{\frac{s}{d}} \equiv 1 \bmod p$. Now conversely, suppose that $a^{\frac{p-1}{d}} \equiv 1 \bmod p$. This means that $g^{s\frac{p-1}{d}} \equiv 1 \bmod p$. Since g is a generator mod p, we have $\mathrm{ord}_p(g) = p-1$, and so in particular, this is possible if and only if $p-1 \mid s\frac{p-1}{d}$. This happens if and only if there is ℓ such that $s\frac{p-1}{d} = (p-1)\ell$. Rearranging, we see this is equivalent to saying that $s = d\ell$ for some ℓ, i.e. $d \mid s$, which is what we wanted.

(b) First, note that 2 is a generator mod 101 (this can be checked by hand), so $6 \equiv 2^s \bmod 101$ for some s. First, let's compute $\mathrm{ord}_{101}(6)$. One can check by hand without too much trouble that $\mathrm{ord}_{101}(6) = 10$. This says $\mathrm{ord}_{101}(2^r) = 10$, and so using the key result that tells us the order of a power, we must have $\frac{100}{\gcd(r,100)} = 10$. This says $\gcd(r, 100) = 10$, and so r is an odd multiple of 10. We have $2^{10} \equiv 14 \bmod 101$, and so checking odd powers of 14 we find $2^{70} \equiv 14^7 \equiv 6 \bmod 101$. Therefore, we wish to solve $2^{5r} \equiv 2^{70} \bmod 101$, which is equivalent to solving $5r \equiv 70 \bmod 100$. Dividing everything by 5, this is the same as saying $r \equiv 14 \bmod 20$, so $r \equiv 14, 34, 54, 74, 94 \bmod 101$ are the 5 different solutions to $5r \equiv 70 \bmod 100$. This yields $x \equiv 2^{14}, 2^{34}, 2^{54}, 2^{74}, 2^{94} \bmod 101$ as our solutions to $x^5 \equiv 6 \bmod 101$.

4. On homework 5, you proved for prime p that $(p-1)! \equiv -1 \bmod p$. Using the fact that there is a generator mod p, give an alternate proof of this result.

Solution: Let g be a generator mod p. Then for any $1 \leq a \leq p-1$, we have $a = g^k \bmod p$ for some unique choice $1 \leq k \leq p-1$. Taking the product over all such values of a is the same thing as taking the product over all such values of k, so we have $(p-1)! = \prod_{a=1}^{p-1} a \equiv \prod_{k=1}^{p-1} g^k \equiv g^{\sum_{k=1}^{p-1} k} \equiv g^{\frac{p(p-1)}{2}} \bmod p$. Now, $g^{\frac{p(p-1)}{2}} \equiv (g^{\frac{p-1}{2}})^p \bmod p$ and because g is a generator, we must have $g^{\frac{p-1}{2}} \equiv -1 \bmod p$, because $g^{\frac{p-1}{2}}$ satisfies $x^2 \equiv 1 \bmod p$ which we know has as it's only solutions $x \equiv \pm 1 \bmod p$. Finally, since p is odd, $(g^{\frac{p-1}{2}})^p \equiv (-1)^p \equiv -1 \bmod p$, so piecing everything together yields $(p-1)! \equiv -1 \bmod p$ as desired.

5. Let p be an odd prime. Prove that -1 is a square mod p if and only if $p \equiv 1 \bmod 4$.

Solution: The forward direction was proven in problem 6(a) of homework 7. For the other direction, suppose that $p \equiv 1 \bmod 4$ and let g be a generator mod p. Then $(g^{\frac{p-1}{4}})^2 \equiv g^{\frac{p-1}{2}} \equiv -1 \bmod p$, which says that -1 is a square mod p.

6. Let p be an odd prime and let $k \geq 0$ be an integer. Prove that

$$1^k + 2^k + \ldots + (p-1)^k \equiv \begin{cases} 0 \bmod p & p-1 \nmid k \\ -1 \bmod p & p-1 \mid k \end{cases}$$

Solution: Let g be a generator mod p. Then for any $1 \leq a \leq p-1$ there is a unique choice of i with $1 \leq i \leq p-1$ such that $a \equiv g^i \bmod p$. Therefore, taking the sum over all such powers of a is the same as taking the sum over all such powers of g: $\sum_{a=1}^{p-1} a^k \equiv \sum_{i=1}^{p-1} (g^i)^k \equiv \sum_{i=1}^{p-1} g^{ki} \bmod p$. If $p-1 \mid k$, then $g^k \equiv 1 \bmod p$, and so the sum is $\sum_{i=1}^{p-1} 1 \equiv p-1 \equiv -1 \bmod p$. If $p-1 \nmid k$, Then recognizing the sum as a geometric series by writing it as $\sum_{i=1}^{p-1} (g^k)^i \bmod p$, we find $\sum_{i=1}^{p-1} (g^k)^i \equiv ((g^k)^p - g^k)(g^k - 1)^{-1} \bmod p$. (note: we can divide by $g^k - 1 \bmod p$ precisely when $p-1 \nmid k$, and so the formula for the sum of a geometric series makes sense). Since $(g^k)^p \equiv g^k \bmod p$ by Fermat's little theorem, this yields $\sum_{i=1}^{p-1} (g^k)^i \equiv 0 \bmod p$. This proves what we want.