# Math 322 Fall 2017
# Number Theory HW 5 Solutions
# Due Wednesday, October 4

You may *not* discuss the starred problem with classmates, though you should of course feel free to discuss it with me as much as you like. Linguistic precision is important for this problem.

($\star$) **Starred Problem:** Suppose $p$ is an odd prime and $a$ is a positive integer with $(a, p) = 1$. Show that the congruence $x^2 \equiv a \mod p$ either has no solution, or has exactly two solutions moduo $p$.

(Hint: assume a solution exists. Find another solution. Then prove that there are no more by assuming that $y$ is any other solution and proving it's the one you found. This problem doesn't require anything sophisticated like Hensel's Lemma).

For the remainder of these problems, I encourage you to collaborate with your classmates, as well as to discuss them with me.

1. Find the solutions of $x^2 + x + 34 \equiv 0 \mod 81$.

   **Solution:** We first find solutions modulo 3. We see that the only solution modulo 3 is 1. $f'(x) = 2x + 1$ so $f'(1) = 3 \equiv 0 \mod 3$.

   We wish to lift to slutions modulo 9. We see that $f(1) = 36 \equiv 0 \mod 9$, so modulo 9, the solutions are $1, 4, 7$ by Hensel's Lemma.

   We now want to lift to solutions modulo 27. The derivative is still 0 modulo 3, so we just test one lift of each solution. We see

   $$\begin{aligned} f(1) &= 36 \equiv 9 \not\equiv 0 \mod 27 \\ f(4) &= 54 \equiv 0 \mod 27 \\ f(7) &= 90 \equiv 9 \not\equiv 0 \mod 27. \end{aligned}$$

   Thus the solutions modulo 27 are $4, 13, 22$.

   Now we want to lift to solutions modulo 81. The derivative is still 0, so we test one lift of each solution. We compute

   $$\begin{aligned} f(4) &= 54 \equiv 54 \not\equiv 0 \mod 81 \\ f(13) &= 216 \equiv 54 \not\equiv 0 \mod 81 \\ f(22) &= 378 \equiv 54 \not\equiv 0 \mod 81. \end{aligned}$$

Thus there are no solutions modulo 81.

2. Find all solutions of $x^3 + 8x^2 - x - 1 \equiv 0 \mod 1331$. (Hint: $1331 = 11^3$).

   **Solution:** We start by computing solutions modulo 11. By trial and error we see the only solutions modulo 11 are 4 and 5. We have $f'(x) = 3x^2 + 16x - 1$, so $f'(4) = 48 + 64 - 1 = 111 \equiv 1 \mod 11$ and $f'(5) = 75 + 80 - 1 = 154 \equiv 0 \mod 11$. We handle the two cases separately.

   Since $f'(4) \equiv 1 \not\equiv 0 \mod 11$, there is a unique solution modulo 121 and modulo 1331. We see the multiplicative inverse of $f(4)$ modulo 11 is again 1. By theorem we have

   $$\begin{aligned} r_1 &\equiv 4 \mod 11 \\ r_2 &\equiv r_1 - f(r_1)(f'(r_1))^{-1} = 4 - 187 \cdot 1 = -183 \equiv 59 \mod 121 \\ r_3 &\equiv r_2 - f(r_2)(f'(r_1))^{-1} = 59 - f(59) \cdot 1 = -233108 \equiv 1148 \mod 1331. \end{aligned}$$

   Now we look at lifts of 5. We have $f'(5) = 0$, so we just test a lift. We see that $f(5) = 319 \equiv 77 \not\equiv 0 \mod 121$, so there are no lifts of 5 to solutions modulo 121–and thus no lifts to solutions modulo 1331.

   Thus the only solution to $f(x) \equiv 0 \mod 1331$ is $x \equiv 1148 \mod 1331$.

3. Find all solutions to $x^5 + x - 6 \equiv 0 \mod 144$.

   **Solution:** 144 is not a prime power; it has prime factors 2 and 3. Thus we will find solutions to $f(x) = x^5 + x - 6 \equiv 0$ modulo 9 and 16, and then use the Chinese Remainder Theorem to combine those results.

   We see that $f(0) = -6 \equiv 0 \mod 2$ and $f(1) = -4 \equiv 0 \mod 2$.

   $f'(x) = 5x^4 + 1$, so $f'(0) = 1$. Thus by formula we have

   $$\begin{aligned} r_1 &\equiv 0 \mod 2 \\ r_2 &\equiv r_1 - f(r_1)(f'(r_1))^{-1} = 0 - (-6) \cdot 1 = 6 \equiv 2 \mod 4 \\ r_3 &\equiv r_2 - f(r_2)(f'(r_1))^{-1} = 2 - f(2) \cdot 1 = 2 - 28 = -26 \equiv 6 \mod 8 \\ r_4 &\equiv r_3 - f(r_3)(f'(r_1))^{-1} = 6 - f(6) \cdot 1 = -7770 \equiv 6 \mod 16. \end{aligned}$$

   Similarly $f'(1) = 6 \equiv 0 \mod 2$. Thus either 1 has two lifts or zero to solutions mod 4. We see $f(1) = -4 \equiv 0 \mod 4$ so 1 and 3 are both solutions modulo 4. The derivative is still zero, so we check both of these mod 8; we have $f(1) = -4 \not\equiv 0 \mod 8$, but $f(3) = 240 \equiv 0 \mod 8$, so 1 is not a solution modulo 8 and 3 is. We check both lifts of 3; we see $f(3) = 240 \equiv 0 \mod 16$, and $f(11) = 161056 \equiv 0 \mod 16$.

   Thus the solutions to $f(x) \equiv 0 \mod 16$ are $x \equiv 3, 6, 11 \mod 16$.

   Now let's work on finding solutions modulo 9. Modulo 3 we see that $f(0) = -6 \equiv 0 \mod 3, f(1) = -4 \not\equiv 0 \mod 3, f(2) = 28 \not\equiv 0 \mod 3$. Thus the only solution modulo 3 is $x \equiv 0 \mod 3$. $f'(0) = 1 \not\equiv 1 \mod 3$ so there is a unique lift to a solution modulo 9. By lemma we have

   $$\begin{aligned} r_1 &\equiv 0 \mod 3 \\ r_1 &\equiv r_1 - f(r_1)(f'(r_1))^{-1} = 0 - (-6) \cdot 1 = 6 \equiv 6 \mod 9. \end{aligned}$$

Thus the unique solution modulo 9 is $x \equiv 6 \mod 9$.

Now we can combine these results using the Chinese Remainder Theorem. Since our bases are always 16 and 9 we always have

$$\begin{aligned} M_1 &= 9 \equiv 9 \mod 16 & \qquad y_1 &\equiv 9 \mod 16 \\ M_2 &= 16 \equiv 7 \mod 9 & \qquad y_2 &\equiv 4 \mod 9 \end{aligned}$$

Then when $x \equiv 3 \mod 16$ and $x \equiv 6 \mod 9$ we have

$$x \equiv 3 \cdot 9 \cdot 9 + 6 \cdot 16 \cdot 4 = 627 \equiv 51 \mod 144.$$

When $x \equiv 6 \mod 16$ and $x \equiv 6 \mod 9$ then we have

$$x \equiv 6 \cdot 9 \cdot 9 + 6 \cdot 16 \cdot 4 = 870 \equiv 6 \mod 144$$

which is *exactly what you should expect*. When $x \equiv 11 \mod 16$ and $x \equiv 6 \mod 9$ then we have

$$x \equiv 11 \cdot 9 \cdot 9 + 6 \cdot 16 \cdot 4 = 1275 \equiv 123 \mod 144.$$

Thus $f(x) \equiv 0 \mod 144$ if and only if $x \equiv 6, 51, 123 \mod 144$.