

18.781: Ideas for solutions to problem set 5

2.6 (8) Use Hensel's lemma with $f(X) = 1000X - 1$. Note that $f'(X) = 1000$, and hence $f'(a)$ is not congruent to zero mod 101 for any a prime to 101. To solve the equation $f(X) \equiv 0 \pmod{101^3}$, note first that $1000 \equiv -10 \pmod{101}$, and hence $f(10) \equiv -100 - 1 \equiv 0 \pmod{101}$. To get a solution mod 101^2 , note that

$$-\frac{f(10)}{101} = -\frac{9999}{101} = 99,$$

and hence Hensel's lemma tells us that if

$$t_2 = -10(99) = -990 \equiv -81 \pmod{81},$$

then $a_2 = 10 - 101 * 81 = -8171$ is a solution of $f(X) \equiv 0 \pmod{101^2}$. Repeating the algorithm to get a solution mod 101^3 , let

$$t_3 = 10(8171001)/101^2 = 8010.$$

Then

$$a_3 = -8171 + (101^2)8010 = 81701839$$

is a solution to $f(X) \equiv 0 \pmod{101^3}$.

2.6 (10) Let $f(X) = X^2 - a$. Then $f'(a) = 2a$. If p is odd and $(a, p) = 1$, then $2a$ is not congruent to zero modulo p , and hence the result follows by induction using Hensel's lemma.

2.7 (3) For any x , $X^{14} \equiv X^2 \pmod{13}$ by Euler's theorem, and hence for any X , $X^{14} + 12X^2 \equiv 0 \pmod{13}$ if and only if $X^2 + 12X^2 = 13X^2 \equiv 0 \pmod{13}$. Since this last congruence holds for all X , the original congruence has 13 solutions.

2.7 (10) This was perhaps a silly question to have on the homework, but because of its relation to the midterm question it was included. Note first that the book denotes the sum

$$\sum_{j=1}^{p-1} \frac{(p-1)!}{j}$$

by σ_{p-2} (defined on the bottom of page 95). Thus finding a common denominator we have

$$1 + \frac{1}{2} + \dots + \frac{p-1}{p} = \frac{\sigma_{p-2}}{(p-1)!}.$$

Let $g = (\sigma_{p-2}, (p-1)!)$. Then by definition, $a = \sigma_{p-2}/g$. Since $g|(p-1)!$, g is prime to p , and hence $a \equiv 0 \pmod{p^2}$ if and only if $\sigma_{p-2} \equiv 0 \pmod{p^2}$. The result therefore follows from Wolstenholme's congruence on page 96.

2.8 (13) Since the set $\{1^k, \dots, (p-1)^k\}$ contains $p-1$ elements prime to p , it is a reduced residue system if and only if for any two i and j with $1 \leq i < j \leq p-1$, the numbers i^k and j^k are not congruent modulo p .

If $(k, p-1) = 1$, then by exercise 4 in 2.5, there exists an integer \bar{k} so that $a^{k\bar{k}} \equiv a \pmod{p}$ for all integers a . This implies that i^k and j^k cannot be congruent mod p , for if they were we would have

$$i \equiv i^{k\bar{k}} \equiv (i^k)^{\bar{k}} \equiv (j^k)^{\bar{k}} \equiv j \pmod{p},$$

which contradicts our assumption that i is not congruent to $j \pmod{p}$.

Conversely, suppose ℓ is a positive common factor of k and $p - 1$, and let $n = (p - 1)/\ell$. Then if g is an element of order $p - 1 \pmod{p}$, the number g^n is not congruent to 1 modulo p , by $g^{nk} = g^{(p-1)(k/\ell)} \equiv 1 \pmod{p}$. This implies that the unique number $i \in \{1, \dots, p - 1\}$ which is congruent to $g^n \pmod{p}$ has the property that $i^k \equiv 1^k \pmod{p}$. Hence the set $\{1, \dots, p - 1\}$ must not be a reduced residue system in this case.

2.8 (14) If $a\bar{a} \equiv 1 \pmod{p}$, then we must have $(a, p) = 1$. Since the order of \bar{a} depends only on the congruence class of \bar{a} , it therefore suffices to prove the second statement. If $a \equiv g^i \pmod{p}$, then

$$a(g^{p-1-i}) \equiv g^i g^{p-1-i} \equiv g^{p-1} \equiv 1 \pmod{p},$$

and from this it follows that $\bar{a} \equiv g^{p-1-i} \pmod{p}$, since $(a, p) = 1$ and hence the set of elements with $a\bar{a} \equiv 1 \pmod{p}$ forms a congruence class. To see that the order of \bar{a} is equal to h , note that by lemma 2.33, the order h of g^i is equal to the smallest number for which $p - 1 | hi$. Similarly, the order \bar{h} of \bar{a} is the smallest number such that $p - 1 | \bar{h}(p - 1 - i)$. But $p - 1$ divides $\bar{h}(p - 1 - i)$ if and only if $p - 1$ divides $-\bar{h}i$, and so it follows that $h = \bar{h}$.

2.8 (22) Since the set $\{g, g^2, \dots, g^{p-1}\}$ forms a reduced residue system, there exists for each $i \in \{1, \dots, p - 1\}$ a unique k so that $i \equiv g^k \pmod{p}$. It follows that

$$(p - 1)! \equiv gg^2g^3 \cdots g^{p-1} \pmod{p}.$$

Since

$$1 + 2 + 3 + \cdots + p - 1 = \frac{p(p - 1)}{2},$$

we have

$$gg^2g^3 \cdots g^{p-1} \equiv g^{p(p-1)/2} \pmod{p}.$$

By Fermat's theorem, this in turn is congruent to $g^{(p-1)/2}$, which is congruent to -1 modulo p since g has order $p - 1$.

3.1 (3) This is a direct computation. The squares mod 13 are $\{1, 3, 4, 9, 10, 12\}$, and the squares mod 7 are $\{1, 2, 4\}$.

3.1 (5) This is again a direct computation. We have $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 = 5$, and $(\pm 5)^2 = 3$. To find the solutions modulo 11^2 use Hensel's lemma.

3.1 (7) (d) and (h) are the only ones which have solutions and they each have 2. Note that each of these equations has either 2 or 0 solutions by theorem 2.37. To check whether each has a solution or not compute the quadratic residue symbol using theorem 3.3 and theorem 3.1 part (5).