

### 18.781: Ideas for solutions to problem set 3

**2.1 (17)** To see that  $61! + 1 \equiv 63! + 1 \pmod{71}$ , it suffices to show that  $63 \cdot 62 \equiv 1 \pmod{71}$ . But  $63 \equiv -8 \pmod{71}$  and  $62 \equiv -9 \pmod{71}$ , so

$$63 \cdot 62 \equiv (-8)(-9) \equiv 72 \equiv 1 \pmod{71}.$$

To show that  $63! + 1 \equiv 0 \pmod{71}$ , note that by Wilson's theorem

$$70! = (63!)(64)(65)(66)(67)(68)(69)(70) \equiv -1 \pmod{71}.$$

Hence it is enough to show that

$$(64)(65)(66)(67)(68)(69)(70) \equiv 1 \pmod{71}.$$

But

$$\begin{aligned} (64)(65)(66)(67)(68)(69)(70) &\equiv (-7)(-6)(-5)(-4)(-3)(-2)(-1) \equiv (-29)(11)(2) \equiv -58 \cdot 11 \\ &\equiv 13 \cdot 11 \equiv 143 \equiv 1 \pmod{71}. \end{aligned}$$

**2.1 (23)** By 2.7, it is enough to show that  $i - 1$  divides 12 for  $i = 2, 3, 5, 7, 13$ . This is clear.

**2.1 (45)** Since  $k \in [1, p - 1]$ ,  $k!$  is prime to  $p$  so it suffices to show that  $k! \binom{p}{k}$  is congruent to 0 modulo  $p$ . But

$$k! \binom{p}{k} = p(p-1) \cdots (p-k+1)$$

which is evidently divisible by  $p$ .

**2.1 (46)** First of all, the condition  $a^p \equiv b^p \pmod{p}$  is by 2.7 equivalent to the condition that  $a \equiv b \pmod{p}$ . Therefore, there exists an integer  $c$  so that  $a = b + pc$ . Now we calculate

$$a^p = (b + pc)^p = \sum_{k=0}^p \binom{p}{k} b^k p^{p-k}.$$

Modulo  $p^2$ , all the terms with  $k < p - 1$  are congruent to zero modulo  $p$ , so we have

$$a^p \equiv b^p + \binom{p}{p-1} p \pmod{p}.$$

By the previous exercise,  $\binom{p}{p-1} \equiv 0 \pmod{p}$ , so we have

$$\binom{p}{p-1} p \equiv 0 \pmod{p}$$

and the result follows.

**2.2 (3)** Let  $r_1, \dots, r_m$  be a complete residue system for  $m$ . Then by assumption  $f(r_i) \equiv 0 \pmod{m}$  for all  $i$ . On the other hand, if  $n$  is any integer whatsoever, there exists a  $r_i$  and an integer  $c$  so that  $n = r_i + cm$ . By 2.2,  $f(n) \equiv f(r_i) \equiv 0 \pmod{m}$ .

**2.2 (5)** This is an application of 2.17.

- (a) No solutions since  $(20, 30) = 10$  which does not divide 4.
- (b) No solutions again since  $(20, 4) = 4$  which does not divide 30.
- (c) This is more complicated. We use the euclidian algorithm

$$400 = 353 + 47$$

$$\begin{aligned} 353 &= 7 * 47 + 24, \\ 47 &= 24 + 23. \\ 24 &= 23 + 1. \end{aligned}$$

Going back up we find that

$$1 = 24 - 23 = 2 * 24 - 47 = 2 * 353 - 15 * 47 = 17 * 353 - 15 * 400.$$

Therefore  $(400, 353) = 1$  and we know that a solution exists. Moreover, we know that all the solutions are given by  $17 * 254$  plus multiples of 400.

**2.2 (14)** We have

$$\binom{p^\alpha}{k} = \frac{p^\alpha(p^\alpha - 1) \cdots (p^\alpha - k + 1)}{k(k-1) \cdots 2 \cdot 1} = \binom{p^\alpha - 1}{k-1} \frac{p^\alpha}{k}.$$

Write  $k = p^\beta k'$  with  $(k', p) = 1$ . Then since  $k < p^\alpha$  we must have  $\beta < \alpha$ . Moreover, since  $k'$  is prime to  $p$ ,

$$\binom{p^\alpha - 1}{k-1} \frac{p^\alpha}{k} \equiv 0 \pmod{p}$$

if and only if

$$k' \binom{p^\alpha - 1}{k-1} \frac{p^\alpha}{k} = \binom{p^\alpha - 1}{k-1} p^{\alpha-\beta} \equiv 0 \pmod{p},$$

which holds since  $\alpha - \beta > 0$ .

**2.2 (17)** Multiplying both sides of the equation by  $(1-x)^p$ , we get

$$(1-x)(1+x+\cdots+x^{p-1}) = (1-x)^p(1+c_1x+c_2x^2+\cdots).$$

Multiplying out the left hand side we get

$$(1) \quad 1 - x^p = (1-x)^p(1+c_1x+c_2x^2+\cdots).$$

On the other hand, we have

$$(1-x)^p = \sum_{i=0}^p (-1)^i \binom{p}{i} x^i.$$

Therefore, when we multiply out the right hand side, we see that the coefficient of  $x^i$  is equal to  $c_i$  plus integers with factors  $\binom{p}{i}$  with  $0 < i < p$ . For example, the coefficient of  $x^3$  is

$$c_3 - \binom{p}{1} c_2 + \binom{p}{2} c_1 - \binom{p}{3}.$$

Now by exercise (2.1 (14)), the numbers  $\binom{p}{i}$  are zero modulo  $p$ , so we see that the coefficient of  $x^i$  when we multiply out the right hand side of (1) is congruent to  $c_i$ . Since the left hand side has no  $x^i$  term it follows that  $c_i \equiv 0$  modulo  $p$ .