Math 345/504
2–28–2018

Solutions to Problem Set 12

1. Simplify $51^{163} \pmod{83}$ to a number in the range $\{0, 1, \ldots 82\}$.

   By Fermat's theorem, $51^{82} = 1 \pmod{83}$. So

   $$\begin{aligned} x &= 51^{163} \pmod{83} \\ x &= 51^{82} \cdot 51^{81} \pmod{83} \\ x &= 51^{81} \pmod{83} \\ 51x &= 51^{82} \pmod{83} \\ 51x &= 1 \pmod{83} \end{aligned}$$

   I need to find $51^{-1} \pmod{83}$.

83	-	13
51	1	8
32	1	5
19	1	3
13	1	2
6	2	1
1	6	0

   $$\begin{aligned} 8 \cdot 83 + (-13) \cdot 51 &= 1 \\ (-13) \cdot 51 &= 1 \pmod{83} \\ 70 \cdot 51 &= 1 \pmod{83} \end{aligned}$$

   Hence, $51^{-1} = 70 \pmod{83}$. Thus,

   $$\begin{aligned} 70 \cdot 51x &= 70 \cdot 1 \pmod{83} \\ x &= 70 \pmod{83} \end{aligned}$$

   □

---

2. Simplify $\dfrac{36!}{17} \pmod{37}$ to a number in the range $\{0, 1, \ldots, 36\}$.

   By Wilson's theorem, $36! = -1 \pmod{37}$. So

   $$\begin{aligned} x &= \frac{36!}{17} \pmod{37} \\ 17x &= 36! = -1 \pmod{37} \end{aligned}$$

37	-	13
17	2	6
3	5	1
2	1	1
1	2	0

$$1 = (17, 37) = (-13) \cdot 17 + 6 \cdot 37.$$

It follows that $17^{-1} = 24 \pmod{37}$, so

$$\begin{aligned} 24 \cdot 17x &= 24 \cdot (-1) \pmod{37} \\ x &= -24 = 13 \pmod{37} \quad \square \end{aligned}$$

---

3. Simplify $85! \pmod{89}$ to a number in the range $\{0, 1, \ldots 88\}$.

   Note: 89 is prime.

   By Wilson's theorem, $88! = -1 \pmod{89}$.

$$\begin{aligned} x &= 85! \pmod{89} \\ 86 \cdot 87 \cdot 88x &= 86 \cdot 87 \cdot 88 \cdot 85! \pmod{89} \\ 86 \cdot 87 \cdot 88x &= 88! \pmod{89} \\ (-3) \cdot (-2) \cdot (-1)x &= -1 \pmod{89} \\ 6x &= 1 \pmod{89} \end{aligned}$$

   Now $6^{-1} = 15 \pmod{89}$, so

$$\begin{aligned} 15 \cdot 6x &= 15 \cdot 1 \pmod{89} \\ x &= 15 \pmod{89} \quad \square \end{aligned}$$

The worst helplessness is forgetting there is help. - James Richardson