# MA352 – Pset 3

Jonathan Lam

April 16, 2020

**Thief gang** *A gang of 19 thieves has a pile of coins containing fewer than 8000 coins. They have to divide the pile evenly but there are 9 coins left over. As a result, a fight breaks out and one of the thieves is killed. They try to divide the pile again, and now they have 8 coins left over. Again, they fight, and again, one of the thieves dies and once more, they try to divide the pile but now they have 3 coins left.*

1. *How many coins are in the pile?*

$$x \equiv 9 \pmod{19}$$

$$x \equiv 8 \pmod{18}$$

$$x \equiv 3 \pmod{17}$$

(Let the $i$-th congruence relation is of the form $x \equiv a_i \pmod{n_i}$.)

$$N = \prod_{i=1}^{3} n_i = 5814$$

The solution to this congruence relation $(\bmod N)$ is:

$$x = \left[\sum_{i=1}^{3} a_i y_i z_i\right] \bmod N$$

where $y_i = N/n_i$ and $z_i = y_i^{-1} \bmod n_i$. Solving for $y_i$ values by division and $z_i$ by the extended Euclidean algorithm:

$$y_1 = 18 \times 17 = 306$$

$$z_1 = 306^{-1} \bmod 19$$

(Extended Euclidean algorithm:)

$$306 z_1 \equiv 1 \bmod 19$$

$$306 z_1 + 19w = 1$$

$$306 = 19 \times 16 + 2, \qquad 2 = 306 - 19 \times 16$$
$$19 = 2 \times 9 + 1, \qquad 1 = 19 - 2 \times 9$$

$$1 = 19 \times 1 - (306 - 19 \times 16) \times 9 = 19 \times 145 + 309 \times (-9)$$
$$z_1 \equiv -9 \equiv 10 \pmod{19}$$

Use the same method to solve for $y_2$, $z_2$, $y_3$, $z_3$ (not shown here):

$$y_2 = 323, \qquad z_2 = 17$$
$$y_3 = 342, \qquad z_3 = 9$$

$$x = \sum_{i=1}^{3} a_i y_i z_i = 9 \times 306 \times 10 + 8 \times 323 \times 17 + 3 \times 342 \times 9 = 80702$$
$$x \mod 5814 = 5120$$

Since the next value of $x$ that would solve this system of congruences would be $2 \times 5120 = 10240 > 8000$, this is the unique solution of $x$.

2. *If they continue this process of fighting, losing one thief and redividing, how man thieves will be left when the pile is finally divided evenly with no remainder?*
   Since $16|5120$, 16 thieves will be left.

**Conductor** .

1. *Find* $\gcd(5, 8)$. Using (extended) Euclidean algorithm:

$$8 = 5 \times 1 + 3, \qquad 3 = 8 - 5 \times 1$$
$$5 = 3 \times 1 + 2, \qquad 2 = 5 - 3 \times 1$$
$$3 = 2 \times 1 + 1, \qquad 1 = 3 - 2 \times 1$$
$$2 = 1 \times 2 + 0$$

   Thus

$$\gcd(5, 8) = 1$$

2. *Find* $x$, $y$ *s.t.* $5x + 8y = \gcd(5, 8)$. Using equations from the previous question:

$$\begin{aligned} 1 &= 3 \times 1 - 2 \times 1 \\ &= 3 \times 1 - (5 - 3 \times 1) \times 1 \\ &= 3 \times 2 + 5 \times (-1) \\ &= (8 - 5 \times 1) \times 2 + 5 \times (-1) \\ &= 8 \times 2 + 5 \times (-3) \end{aligned}$$

   Thus a particular solution is:

$$(x, y) = (-3, 2)$$

   and the general solution is

$$(x, y) = (-3 - 8t, 2 + 5t), \ t \in \mathbb{Z}$$

3. *It is a fact that given two nonnegative integers* $a$, $b$ *where* $\gcd(a,b) = 1$*, there is always a point beyond which every integer is representable as* $ax + by$ *where* $x$ *and* $y$ *are both nonnegative integers. The least such result is denoted* $\text{cond}(a,b)$*. Find* $\text{cond}(5,8)$*.*

   Since $\gcd(5,8) = 1$, we can use the result derived in the next section.

   $$\text{cond}(5,8) = (5-1)(8-1) = 28$$

4. *Find the general formula for* $\text{cond}(a,b)$ *where* $\gcd(a,b) = 1$*.*

   Since $\gcd(a,b) = 1$, we know that there are infinitely many solutions to the linear Diophantine equation:

   $$ax + by = c, \; c \in \mathbb{Z}$$

   If $(x,y) = (x_0, y_0)$ is a particular solution, then we know that other particular solutions are of the form $(x,y) = (x_0 + bt, y_0 - at), \; t \in \mathbb{Z}$. Thus, a number cannot be represent by a positive tuple $(x,y)$ if $x_0 < 0$ and $y_0 < a$ (or, alternatively, if $y_0 < 0$ and $x < b$). The largest of such would be when $x = -1$, $y = a - 1$ (or, alternatively, when $x = b - 1$, $y = -1$; both give the same answer). If we plug this into the Diophatine equation, this gives us the largest integer *not* representable by a positive tuple, so $\text{cond}(a,b)$ is this number plus one:

   $$\text{cond}(a,b) = (a(-1) + b(a-1)) + 1 = -a + ab - b + 1 = (a-1)(b-1)$$

5. *In the United Kingdom, chicken nuggets are sold in packs of 9 or 20. What is the largest number of chicken nuggets that you cannot buy?*

   The answer is $\text{cond}(9,20) - 1$. Since $\gcd(9,20) = 1$, we can use the result from the previous section.

   $$\text{cond}(9,20) - 1 = (9-1)(20-1) - 1 = 151$$