Fourth Exercise Session: 20/4

Themes: Number theory

Relevant Chapters: Vol.1: 3

1. Computer GCD and LCM of 147 and 336, both with and without Euclid's algorithm.

2. Factorise 1615 and determine the smallest prime greater than this.

3. **(a)** Compute the general solution to the Diophantine equation $73x + 17y = 2000$.
(b) Determine all positive solutions and the solution for which $|x| + |y|$ is minimal.
(c) What is the general solution to $73x - 17y = 2000$? How many positive solutions are there to this equation ?
(d) For which $c \in \mathbb{Z}$ does the Diophantine equation $147x + 336y = c$ have a solution ?

4. Prove that, if $p > 3$ is a prime, then $p^2 \equiv 1 \pmod{24}$.

Solutions

1. To compute GCD without Euclid's algorithm we factorise each number and pluck out the common prime factors.

$$147 = 3 \cdot 7^2, \quad 336 = 2^4 \cdot 3 \cdot 7 \quad \Rightarrow \text{ GCD}(147,\, 336) = 3 \cdot 7 = 21.$$

If we instead used Euclid's algorithm, it would proceed as follows:

$$\begin{aligned} 336 &= 2 \cdot 147 + 42, \\ 147 &= 3 \cdot 42 + 21, \\ 42 &= 2 \cdot 21 + 0. \end{aligned}$$

As regards the LCM, note that in general,

$$\text{GCD}\left(\prod_{i=1}^{k} p_i^{\alpha_i},\, \prod_{i=1}^{k} p_i^{\beta_i}\right) = \prod_{i=1}^{k} p_i^{\min\{\alpha_i,\,\beta_i\}} \tag{1}$$

whereas

$$\text{LCM}\left(\prod_{i=1}^{k} p_i^{\alpha_i},\, \prod_{i=1}^{k} p_i^{\beta_i}\right) = \prod_{i=1}^{k} p_i^{\max\{\alpha_i,\,\beta_i\}} \tag{2}$$

Hence, from the prime factorisations it follows directly that

$$\text{LCM}(147,\, 336) = 2^4 \cdot 3 \cdot 7^2 = 2352.$$

If we'd instead used Euclid to compute GCD, then we can observe that it follows from (1) and (2) that, for any two integers a and b,

$$\text{GCD}(a,\, b) \cdot \text{LCM}(a,\, b) = ab.$$

Thus,

$$21 \cdot \text{LCM}(147,\, 336) = 147 \cdot 336 \quad \Rightarrow \quad \text{LCM}(147,\, 336) = \frac{147 \cdot 336}{21} = 2352.$$

2. (i)

$$1615 = 5 \cdot 323 = 5 \cdot 17 \cdot 19.$$

(ii) 1616 obvously isn't prime because it's even. 1617 isn't prime because the digit sum is 15, which is divisible by 3. 1618 isn't prime because it's even. It turns out that 1619 is prime. To verify this, it suffices to check that it is not divisible by any prime up to $\sqrt{1619} = 40, ...$, in other words any prime up to 37. Just do it !

3. (a) *Step 1:* Euclid forwards.

$$\begin{aligned} 73 &= 4 \cdot 17 + 5, \\ 17 &= 3 \cdot 5 + 2, \\ 5 &= 2 \cdot 2 + 1. \end{aligned}$$

The GCD is 1, which divides 2000, hence we know the Diophantine equation has a solution.

Step 2: Euclid backwards to find one solution to $ax + by = d$.

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(17 - 3 \cdot 5) \\ &= 7 \cdot 5 - 2 \cdot 17 \\ &= 7(73 - 4 \cdot 17) - 2 \cdot 17 \\ &= 7 \cdot 73 - 30 \cdot 17. \end{aligned}$$

Hence we can take $x_0 = 7$, $y_0 = -30$.

Step 3: Insert in formula for general solution.

$$\begin{aligned} x &= mx_0 - \left(\frac{b}{d}\right) n, \\ y &= my_0 + \left(\frac{a}{d}\right) n, \quad n \in \mathbb{Z}. \end{aligned}$$

Here $m = 2000$, $a = 73$, $b = 17$, $d = 1$. Thus,

$$\begin{aligned} x &= 14000 - 17n, \\ y &= -60000 + 73n, \quad n \in \mathbb{Z}. \end{aligned} \tag{3}$$

(b) A positive solution satisfies

$$\begin{aligned} x > 0 \Rightarrow 14000 - 17n > 0 \Rightarrow n < \frac{14000}{17} = 823, ... \Rightarrow n \leq 823 \\ y > 0 \Rightarrow -60000 + 73n > 0 \Rightarrow n > \frac{60000}{73} = 821, ... \Rightarrow n \geq 822. \end{aligned}$$

Hence there are two positive solutions corresponding to $n = 822$ and $n = 823$. We can be a little efficient in computing them. First insert $n = 822$ into the formula for x to get $x = 14000 - 17(822) = 26$. Then insert this into the Diophantine equation itself to get $y = \frac{2000-73(26)}{17} = \frac{102}{17} = 6$.

Thus the first positive solution is $(26,\ 6)$. The second one is got by increasing n by one which, by (3), must have the effect of decreasing x by 17 and increasing y by 73. Hence the second positive solution is $(9,\ 79)$.

Finally it is pretty clear that $(26,\ 6)$ is the solution which minimises $|x| + |y|$.

(c) One just replaces y by $-y$ in (3), which leads to

$$\begin{aligned} x &= 14000 - 17n, \\ y &= 60000 - 73n, \quad n \in \mathbb{Z}. \end{aligned} \tag{4}$$

This time there will be infinitely many positive solutions. To see this, start for example from the solution $(26,\ 6)$ in (3). This corresponds to the solution $(26,\ -6)$ in (4). If we now decrease n, then x will increase in steps of 17 and y will also increase in steps of 73. Hence every solution corresponding to $n \leq 821$ is positive.

(d) In Q.1 we computed GCD$(147,\ 336) = 21$. Hence the equation has a solution if and only if c is a multiple of 21.

4. Note the following consequence of FTA:

Let a and b be any two integers satisfying GCD$(a, b) = 1$. Then for any integer c,

$$ab \,|\, c \quad \Leftrightarrow \quad a \,|\, c \,\wedge\, b \,|\, c.$$

So a number is divisible by 24 if and only if it is divisible by both 3 and 8. It remains to show that this is true of $p^2 - 1$, for any prime $p > 3$. We use the fact that $p^2 - 1 = (p-1)(p+1)$.

Divisibility by 3*:* Since p is a prime and greater than 3, it is not a multiple of 3. But amongst any three consecutive integers, there must be a multiple of 3. Since p isn't so, either $p - 1$ or $p + 1$ must be. Hence $p^2 - 1$ will be a multiple of 3.

Divisibility by 8*:* p is odd, hence both $p - 1$ and $p + 1$ are even. Moreover, amongst two consecutive even numbers one must be a multiple of 4. So one of $p \pm 1$ is a multiple of 4 and the other is a multiple of 2, so their product will be a multiple of 8.