Math 114 Discrete Mathematics

Section 3.7, selected answers

D Joyce, Spring 2018

2. Express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

a. 9, 11. The GCD is 1. We need to find 1 as a linear combination of 9 and 11. These are small enough numbers so we can do it by searching. We need to find a multiple of 9 that is one more or less than a multiple of 11. The multiples of 9 are 9, 18, 27, 36, 45. Stop. 45 is 1 more than 44. That is $9 \cdot 5 = 1 + 4 \cdot 11$. Thus,

$$1 = (-5) \cdot 9 + 4 \cdot 11$$

expresses the GCD of 9 and 11, namely, 1, as a linear combination of 9 and 11.

b. 33, 44. The GCD is 11, but 11 is $44 - 33$, thus

$$11 = (-1) \cdot 33 + 1 \cdot 44$$

expresses 11 as a linear combination of 33 and 44.

c. 35, 78. The numbers are getting larger. A search would work, but the general method is probably just as fast. We'll use the Euclidean algorithm keeping track of our computations and build the answer from that.

$$\begin{aligned} 78 &= 2 \cdot 35 + 8 \\ 35 &= 4 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

Now, build up the answer starting with the last equation

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 2 \cdot 3) \\ &= 3 \cdot 3 - 8 \\ &= 3 \cdot (35 - 4 \cdot 8) - 8 \\ &= 3 \cdot 35 - 13 \cdot 8 \\ &= 3 \cdot 35 - 13 \cdot (78 - 2 \cdot 35) \\ &= 29 \cdot 35 - 13 \cdot 78 \end{aligned}$$

6. Find an inverse of 2 modulo 17.

Which multiple of 2 is one more than 17? 2 times 9 equals 18. Thus,

$$2 \cdot 9 \equiv 1 \pmod{17},$$

so 8 is an inverse of 2 modulo 17.

18. Find all solutions to the system of congruences

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

The numbers are small enough to search for answer. The least common multiple of 3, 4, and 5 is 60, so we only have to look for a integer x less than 60 that satisfies all three congruences. Even though it can be done by a search, I'll show here how to solve it with the algorithm given in the text. (There are many others.)

Following the notation in the text,

$$a_1 = 2, a_2 = 1, a_3 = 3,$$

$$m_1 = 3, m_2 = 4, m_3 = 5.$$

Then $m = m_1 m_2 m_3 = 60$. Next,

$$M_1 = m/m_1 = 20, M_2 = m/m_2 = 15, M_3 = m/m_3 = 12.$$

Now we need to find inverses y_k for M_K modulo m_k. First we need y_1 so that $M_1 y_1 \equiv 1 \pmod{m_1}$, that is, $20y_1 \equiv 1 \pmod 3$. $y_1 = 2$ works. Second, solve $M_2 y_2 \equiv 1 \pmod{m_2}$, that is, $15y_2 \equiv 1 \pmod 4$. $y_2 = 3$ works. Third, solve $M_3 y_3 \equiv 1 \pmod{m_3}$, that is, $12y_3 \equiv 1 \pmod 5$. $y_3 = 3$ works.

We get our answer

$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 \\ &= 233 \end{aligned}$$

and we can reduce our answer modulo $m = 60$ to get $x = 53$.

Math 114 Home Page at `http://math.clarku.edu/~djoyce/ma114/`