SOLUTIONS
Math 345
Homework 3
9/25/2017

Exercise 8. Set up a computer program or spreadsheet to compute the $\gcd(a, b)$ for any positive integers a and b. To check that your answer is correct, plug in the values $a = 100$ and $b = 36$, and compare your q and r values to those from lecture.

Now, compute the prime factorizations of the following a and b values (ok to use a calculator), and use those to compute $\gcd(a, b)$. Then plug into your program/spreadsheet to verify your answer. Report how many steps the Euclidean algorithm took in each example (i.e. what is n?)

(a) $a = 242$, $b = 25$;

Answer. We have $242 = 2 \cdot 11^2$ and $25 = 5^2$, so $\gcd(242, 25) = 1$. See spreadsheet for verification. □

(b) $a = 5390$, $b = 504$.

Answer. We have $5390 = 2 \cdot 5 \cdot 7^2 \cdot 11$ and $504 = 2^3 \cdot 3^2 \cdot 7$, so $\gcd(5390, 504) = 2 \cdot 7$. See spreadsheet for verification. □

Exercise 9. Recall from lecture that executing the Euclidean algorithm for $a = 100$ and $b = 36$ gives the following equations:

$$100 = 36 * 2 + 28, \tag{E1}$$
$$36 = 28 * 1 + 8, \tag{E2}$$
$$28 = 8 * 3 + 4, \tag{E3}$$
$$8 = 4 * 2 + 0. \tag{E4}$$

(a) Follow these steps to express 4 as an *integer combination* of 100 and 36, i.e., find (possibly negative) integers x and y such that $100x + 36y = 4$:

(i) Use equation (E3) to express 4 as an integer combination of 8 and 28 (find integers x and y such that $8x + 28y = 4$).

(ii) Use equation (E2) to express 8 as an integer combination of 28 and 36 (find integers x and y such that $28x + 36y = 8$).

(iii) Use equation (E1) to express 28 as an integer combination of 36 and 100 (find integers x and y such that $36x + 100y = 28$).

(iv) Plug your equation from part (ii) into your equation in part (i), expanding and simplifying, to express 4 as an integer combination of 28 and 36 (find integers x and y such that $36x + 28y = 4$).

(v) Plug your equation from part (iii) into your equation in part (iv), expanding and simplifying, to express 4 as an integer combination of 36 and 100 (find integers x and y such that $100x + 36y = 4$).

Answer. Following these steps, we get

$$4 = 28 - 8 * 3, \qquad 8 = 36 - 28 * 1, \qquad \text{and} \qquad 28 = 100 - 36 * 2,$$

so that

$$\begin{aligned} 4 &= 28 - 8 * 3 \\ &= (100 - 36 * 2) - (36 - 28 * 1) * 3 \\ &= 100 - 36 * 2 - 36 * 3 + (100 - 36 * 2) * 3 \\ &= 100(1 + 3) + 36(-2 - 3 - 2 * 3) \\ &= 100(4) + 36(-11). \end{aligned}$$

So $x = 4$ and $y = -11$ is one integer solution to $100x + 36y = 4$ (checked on a calculator). □

(b) Use your computer calculations from Exercise 8(b) to write out the equations for the Euclidean algorithm (like those in (E1)–(E4)). Then use those to write $\gcd(242, 25)$ as an integer combination of 242 and 25, using the same strategy as in part (a).

Answer. The Euclidean algorithm for $a = 242, b = 25$ is

$$242 = 25 * 9 + 17, \tag{0.1}$$
$$25 = 17 * 1 + 8, \tag{0.2}$$
$$17 = 8 * 2 + 1. \tag{0.3}$$

So

$$1 = 17 - 8 * 2, \qquad 8 = 25 - 17 * 1, \qquad \text{and} \qquad 17 = 242 - 25 * 9.$$

Therefore,

$$\begin{aligned}
1 &= 17 - 8 * 2 \\
&= 17 - (25 - 17 * 1) * 2 \\
&= (242 - 25 * 9) - (25 - (242 - 25 * 9) * 1) * 2 \\
&= 242 - 25 * 9 - 25 * 2 + 242 * 2 - 25 * 9 * 2 \\
&= 242(1 + 2) + 25(-9 - 2 - 18) \\
&= 242(3) + 25(-29).
\end{aligned}$$

□

(c) Make an argument justifying the following claim:
For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$.

Proof. The Euclidean algorithm gives

$$\begin{array}{ccccccl}
a & = & b * q_1 & + & r_1 & & \\
b & = & r_1 * q_2 & + & r_2 & & \\
r_1 & = & r_2 * q_3 & + & r_3 & & \\
 & \vdots & & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow & \gcd(a, b) \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow & r_n.
\end{array}$$

Rewriting to solve for the r_i's we get

$$\begin{aligned}
r_1 &= a - b * q_1 \\
r_2 &= b - r_1 * q_2 \\
r_3 &= r_1 - r_2 * q_3 \\
&\vdots \\
r_{n-2} &= r_{n-4} - r_{n-3} * q_{n-2} \\
r_{n-1} &= r_{n-3} - r_{n-2} * q_{n-1}.
\end{aligned}$$

Then starting from the end at r_{n-1} and working our way up, we see that we can plug in successfully prior values of r_i's until we arrive at an expression in $r_0 = b$, $r_{-1} = a$, and the $q_i's$ alone:

$$r_{n-1} = r_{n-3} - r_{n-2} * q_{n-1} = (r_{n-5} - r_{n-4} * q_{n-3}) - (r_{n-4} - r_{n-3} * q_{n-2}) * q_{n-1} = \cdots .$$

Noting that, at every step, we always get an integer combination of the r_i's, we find the desired result by iteration. □

Exercise 10. A number ℓ is called a *common multiple* of positive integers a and b if $a|\ell$ and $b|\ell$. The smallest (positive) such ℓ is called the *least common multiple* of a and b, denoted $\operatorname{lcm}(a,b)$. For example, $\operatorname{lcm}(3,7) = 21$ and $\operatorname{lcm}(12,66) = 132$.

(a) Complete the following table of values (using your program/spreadsheet to compute the gcd)... Try to surmise a relationship between a, b, $\gcd(a,b)$, and $\operatorname{lcm}(a,b)$.

Answer.

a	b	ab	$\gcd(a,b)$	$\operatorname{lcm}(a,b)$
12	8	96	4	24
30	20	600	10	60
68	51	3468	17	204
23	18	414	1	414

It appears that we keep getting $ab = \gcd(a,b)\operatorname{lcm}(a,b)$. □

(b) Give an argument proving that the relationship you found at the end of part (a) is correct for all a and b.

Proof. We claim that $ab = \gcd(a,b)\operatorname{lcm}(a,b)$.

To see why this is true, consider $L = ab/\gcd(a,b)$. We will try to show that this is, indeed, the least common multiple of a and b.

Let $g = \gcd(a,b)$. Then since g is a divisor of both a and b, we have $(a/g), (b/g) \in \mathbb{Z}$, so that

$$L = a(b/g) \quad \text{is an integer multiple of } a,$$

and

$$L = b(a/g) \quad \text{is an integer multiple of } b.$$

So L is a common multiple of a and b.

To see that it is the least such multiple, let m be a positive common multiple; it will suffice to show that $L|m$:

Let $u, v \in \mathbb{Z}$ satisfy $g = ua + vb$ (which we know exist by exercise 9). Since $a|m$ and $b|m$, we have

$$m = ak \quad \text{and } m = b\ell \quad \text{for some } k, \ell \in \mathbb{Z}.$$

Therefore,

$$\begin{aligned} m &= (m/g)g = (m/g)ua + (m/g)vb \\ &= (b\ell/g)ua + (ak/g)vb = \ell u\left(\frac{ab}{g}\right) + kv\left(\frac{ab}{g}\right) \\ &= (\ell u + kv)\left(\frac{ab}{g}\right) = (\ell u + kv)L. \end{aligned}$$

So since $\ell u + kv \in \mathbb{Z}$, we have $L|m$.

Therefore, $L = \operatorname{lcm}(a,b)$. □

(c) Use your result in (b), along with your gcd calculator to lcm(301337, 307829).

Answer. We have gcd(301337, 307829) = 541 (see spreadsheet). So

$$\text{lcm}(301337, 307829) = 301337 * 307829/541 = \boxed{171,460,753}.$$

□

(d) Suppose that $\gcd(a, b) = 18$ and $\text{lcm}(a, b) = 720$. What are the possibilities for the values of a and b?

Answer. If $\gcd(a, b) = 18$, then we must have

$$a = 18a_{\text{div}} \quad \text{and } b = 18b_{\text{div}} \quad \text{for } a_{\text{div}}, b_{\text{div}} \in \mathbb{Z} \text{ with } \gcd(a_{\text{div}}, b_{\text{div}}) = 1.$$

And since $\text{lcm}(a, b) = 720$, we must have

$$720 = a \cdot a_{\text{mult}} \quad \text{and} \quad 720 = b \cdot b_{\text{mult}} \quad \text{for } a_{\text{mult}}, b_{\text{mult}} \in \mathbb{Z} \text{ with } \gcd(a_{\text{mult}}, b_{\text{mult}}) = 1.$$

Then since

$$ab = \gcd(a, b)\text{lcm}(a, b) = (a/a_{\text{div}})(b \cdot b_{\text{mult}}),$$

we have

$$1 = b_{\text{mult}}/a_{\text{div}}, \qquad \text{so that } a_{\text{div}} = b_{\text{mult}}.$$

Similarly, $a_{\text{mult}} = b_{\text{div}}$. Basically, whatever you have to multiply b by to get 720 is what you have to multiply 18 by to get a. (Informally, think of a prime factorization as a (multi)set of primes dividing a number. Then $\gcd(a, b)$ is the intersection of these multisets, $\text{lcm}(a, b)$ is the union, and ab is the disjoint union. We are essentially looking for two multisets whose intersection and unions are defined, and then moving elements outside of the intersection from one set to the other.)

So, in short, we're looking to set a_{div} to any of the divisors of $720/18 = 40 = 2^3 \cdot 5$ (of which there are $4 * 2 = 8$), and then letting

$$a = 18a_{\text{mult}}, \quad \text{and } b = 18b_{\text{mult}} = 18a_{\text{div}} = 18(720/a_{\text{mult}}).$$

Doing this, we get

a	$2 \cdot 3^2$	$2^2 \cdot 3^2$	$2^2 \cdot 3^2$	$2^4 \cdot 3^2$
b	$2^4 \cdot 3^2 \cdot 5$	$2^3 \cdot 3^2 \cdot 5$	$2^2 \cdot 3^2 \cdot 5$	$2 \cdot 3^2 \cdot 5$

a	$2^4 \cdot 3^2 \cdot 5$	$2^3 \cdot 3^2 \cdot 5$	$2^2 \cdot 3^2 \cdot 5$	$2 \cdot 3^2 \cdot 5$
b	$2 \cdot 3^2$	$2^2 \cdot 3^2$	$2^2 \cdot 3^2$	$2^4 \cdot 3^2$

Now, restricting to the cases where $720/a$ and $720/b$ are relatively prime, we have, finally,

a	$2 \cdot 3^2$	$2^4 \cdot 3^2$	$2^4 \cdot 3^2 \cdot 5$	$2 \cdot 3^2 \cdot 5$
b	$2^4 \cdot 3^2 \cdot 5$	$2 \cdot 3^2 \cdot 5$	$2 \cdot 3^2$	$2^4 \cdot 3^2$

□

Exercise 11.

(a) Describe all integer solutions to each of the following equations:

$$105x + 121y = 1 \quad \text{and} \quad 12345x + 67890y = \gcd(12345, 67890)$$

(first find one solution, and go from there).

Answer. Reversing the Euclidean algorithm (see spreadsheet), we get

$$\begin{aligned} 1 &= 7 - 2 * 3 \\ &= (16 - 9 * 1) - (9 - 7) * 3 = 16 - 9 * 4 + 7 * 3 \\ &= (121 - 105) - (105 - 16 * 6) * 4 + (16 - 9) * 3 = 121 - 5 * 105 + 16 * 27 - 9 * 3 \\ &= 121 - 105 * 5 + (121 - 105) * 27 - (105 - 16 * 6) * 3 = 121 * 28 - 105 * 35 + 16 * 18 \\ &= 121 * 28 - 105 * 35 + (121 - 105) * 18 = 121 * 46 + 105 * (-53) \end{aligned}$$

Then all solutions to $105x + 121y = 1$ are of the form

$$x = -53 + 121k \quad \text{and} \quad y = 46 - 105k \quad k \in \mathbb{Z}.$$

We have $\gcd(12345, 67890) = 15$. Again, reversing the Euclidean algorithm (see spreadsheet), we get

$$\begin{aligned} 15 &= 12345 - 6165 * 2 \\ &= 12345 - (67890 - 12345 * 5) * 2 \\ &= 12345 * (11) - 67890 * 2. \end{aligned}$$

Then all solutions to $12345x + 67890y = 15$ are of the form

$$x = 11 + 67890k \quad \text{and} \quad y = -2 - 12345k \quad k \in \mathbb{Z}.$$

□

(b) Show that, for $a, b \in \mathbb{Z}_{\neq 0}$, and any $x, y \in \mathbb{Z}$, that

$$\text{if } d|a \text{ and } d|b \quad \text{then} \quad d|(ax + by).$$

(Do *not* assume that $ax + by = \gcd(a, b)$. There are lots of other integral combinations of a and b.)

Proof. If $d|a$ and $d|b$ then there are $k, \ell \in \mathbb{Z}$ satisfying $a = kd$ and $b = \ell d$. So

$$ax + by = kdx + \ell dy = d(kx + \ell y).$$

So since $(kx + \ell y) \in \mathbb{Z}$, we have $d|(ax + by)$.

□

(c) Suppose that $\gcd(a, b) = 1$. Prove that for every integer c, the equation $ax + by = c$ has a solution in integers x and y.

Proof. If $\gcd(a, b) = 1$, then there are $u, v \in \mathbb{Z}$ satisfying $au + bv = 1$. Multiplying both sides by c we get

$$c = a(cu) + b(cv).$$

So since $cu, cv \in \mathbb{Z}$, setting $x = cu$ and $y = cv$ give us the desired result. □

(d) Now, in general, if $\gcd(a, b) = g$, what integers c come in the form $c = ax + by$?
(See the spreadsheet from lecture–try plugging in different values for a and b and observing which values appear in the table. Then answer in general, and prove your claim.)

Proof. If $\gcd(a, b) = g$, then there are $u, v \in \mathbb{Z}$ satisfying $au + bv = g$. Further, we showed that if $c = ax + by$, then $g|c$. So if c is not a multiple of g, there are no integer solutions to $c = ax + by$. Otherwise $c/g \in \mathbb{Z}$, and so

$$c = (c/g)g = a(cu/g) + b(cv/g)$$

shows that $x = (cu/g)$ and $y = (cv/g)$ gives an integer solution to $c = ax + by$. □

Exercise 12.

(a) Find integers x, y, and z that satisfy the equation

$$6x + 15y + 20z = 1.$$

Answer. First, by the last problem, we know that $6x+15y$ must be a multiple of $\gcd(6, 15) = 3$, and can be any multiple of 3. In particular,

$$3 * 6 - 15 = 3, \qquad \text{so that } 3(6 * 7) + 15(-7) = 3 * 7 = 21.$$

So

$$3(6 * 7) + 15(-7) + 20(-1) = 1.$$

□

(b) Under what conditions on a, b, c is it true that the equation

$$ax + by + cz = 1$$

has an integer solution? (So that $x, y, z \in \mathbb{Z}$.)
Describe a general method of finding a solution when one exists.

Answer. As hinted at in the previous problem, $ax + by = u$ if and only if $u = w\gcd(a, b)$ for $w \in \mathbb{Z}$. And $u\gcd(a, b) + cz = 1$ has a solution if and only if $1 = \gcd(\gcd(a, b), c) = \gcd(a, b, c)$. We can then find it by first finding X and Y such that $Xa + Yb = \gcd(a, b)$, and then finding U and V such that $U\gcd(a, b) + Vc = 1$. Then set $x = XU$, $y = YU$, $z = V$. □

(c) Use your method from (b) to find a solution in integers to the equation

$$155x + 341y + 385z = 1.$$

Answer. First,

$$31 = \gcd(155, 341) = 341 - 2 * 155.$$

Then reversing the Euclidean algorithm for 31 and 385, we get

$$\begin{aligned}
1 &= 3 - 2 = (13 - 5 * 2) - (5 - 3) = 13 - 5 * 3 + 3 \\
&= 385 - 31 * 12 - (31 - 13 * 2) * 3 + 13 - 5 * 2 = 385 - 31 * 15 + 13 * 7 - 5 * 2 \\
&= 385 - 31 * 15 + (385 - 31 * 12) * 7 - (31 - 13 * 2) * 2 = 385 * 8 - 31 * 101 + 13 * 4 \\
&= 385 * 8 - 31 * 101 + (385 - 31 * 12) * 4 = 385 * 12 + 31 * (-149).
\end{aligned}$$

So $155x + 341y + 385z = 1$ has solution

$$x = (-149)(-2), \quad y = (-149)(1), \quad z = 12.$$

□