

**DISCRETE MATHEMATICS
HOMEWORK 5 SOLUTIONS**

1. Most of these weren't too bad, but there may have been exceptions.

- (a) $-31 = 59$ in \mathbb{Z}_{90} because $31 + 59 = 0$ in \mathbb{Z}_{90} .
- (b) There are a couple of approaches to this one. You could just start multiplying and discover by trial and error that $7 \times 4 = 28 = 3$ in \mathbb{Z}_{25} , which means that $3/7 = 4$ in \mathbb{Z}_{25} . You could also discover (either by trial and error or using the methods of the problems below) that $7 \times 18 = 126 = 1$, which means that $1/7 = 18$, so that $3/7 = 3(1/7) = 3(18) = 54 = 4$.
- (c) $\sqrt{-1} = \pm 5 = 5$ or 8 in \mathbb{Z}_{13} , since $5^2 = 8^2 = 12 = -1$ in \mathbb{Z}_{13} .
- (d) This one contained a slight surprise: $\sqrt{4}$ has 4 distinct values in \mathbb{Z}_{16} : any of 2, 6, 10, or 14 square to give 4 in \mathbb{Z}_{16} .
- (e) Here's the arithmetic:

$$\begin{aligned}197191561 &= 98444328 \cdot 2 + 302905 \\98444328 &= 302905 \cdot 325 + 203 \\302905 &= 203 \cdot 1492 + 29 \\203 &= 29 \cdot 7 + 0\end{aligned}$$

The gcd is therefore 29. The occurrence of the historically important dates of 325 (the First Ecumenical Council) and 1492 (the beginning of the European invasion of America) might have suggested to you that your arithmetic was OK.

2. The first and third claims were correct; the second was nonsense.

- (a) If $ab \mid c$, then there is an integer x such that

$$c = (ab)x.$$

This means that $c = a(bx)$. Since b and x are both integers, and since \mathbb{Z} is closed under multiplication, bx is an integer. Thus, for some integer $y = bx$, $c = ay$. In other words, $a \mid c$.

- (b) If $a \mid c$ and $b \mid c$, then it is not in general the case that $ab \mid c$. For instance, let $a = 6$, $b = 4$, and $c = 12$.
- (c) If $a \mid (b + c)$ and $a \mid (b - c)$, then there are integers x and y such that

$$\begin{aligned}ax &= b + c \\ay &= b - c.\end{aligned}$$

Adding these equations gives $a(x + y) = 2b$. Since the integers are closed under addition, $x + y \in \mathbb{Z}$. Thus, $a \mid 2b$. It is not necessarily the case that $a \mid b$. For instance, let $a = 4$, $b = 2$, and $c = 6$.

3. One could use Euclid's algorithm to solve two of these. One could also just mess around and discover that $2 \cdot 311 = 622 = 1$, so that $\frac{1}{2} = 311$; and that $4 \cdot 466 = 1864 = 1$, so that $\frac{1}{4} = 466$.

The last fraction, $\frac{1}{3}$, doesn't exist in \mathbb{Z}_{621} . Why? Because if $\frac{1}{3} = x$ in \mathbb{Z}_{621} , then $3x = 1$ in \mathbb{Z}_{621} , which means that for some $y \in \mathbb{Z}$, $3x = 1 + 621y$, i.e., that for some $y \in \mathbb{Z}$, $3x - 621y = 1$. But $3x - 621y = 3(x - 207y)$. The closure of \mathbb{Z} under multiplication and subtraction tells us that $x - 207y \in \mathbb{Z}$; so that $3 \mid (3x - 621y)$. Obviously $3 \nmid 1$, though; so the Diophantine equation $3x - 621y = 1$ has no integer solutions. In other words, $\frac{1}{3}$ does not exist in \mathbb{Z}_{621} .

4. The first and second of these were familiar. The third was a small but useful stretch.
- (a) To solve the equation $215x - 611y = 1$, we begin by doing Euclid's algorithm in order to be sure a solution will exist. The calculation looks like this:

$$\begin{aligned} 611 &= 215(2) + 181 \\ 215 &= 181(1) + 34 \\ 181 &= 34(5) + 11 \\ 34 &= 11(3) + 1 \\ 11 &= 1(11) + 0 \end{aligned}$$

The gcd is therefore 1; so there should be a solution. To find it, we rewrite the equations from Euclid's algorithm for the remainders:

$$\begin{aligned} 181 &= 611 - 215(2) \\ 34 &= 215 - 181(1) \\ 11 &= 181 - 34(5) \\ 1 &= 34 - 11(3). \end{aligned}$$

We then march up the string of equations, using each equation as a substitution in the next to get

$$\begin{aligned} 1 &= 34 - 11(3) = 34 - [181 - 34(5)](3) = 34(16) - 181(3) \\ &= [215 - 181(1)](16) - 181(3) = 215(16) - 181(19) \\ &= 215(16) - [611 - 215(2)](19) = 215(54) - 611(19). \end{aligned}$$

One solution to the equation is thus $x = 54$, $y = 19$.

To get more solutions, do what we did in class: let $x = 54 + 611t$ and $y = 19 + 215t$ for any integer t . This always produces solutions, since

$$\begin{aligned} 215(54 + 611t) - 611(19 + 215t) &= 215(54) + 215(611t) - 611(19) - 611(215t) \\ &= 215(54) - 611(19) = 1. \end{aligned}$$

To show that every solution has this form was probably a stretch at the time of the test, though we had given a geometric argument in class that you could have used here. With our current state of knowledge, though, we can do better. Let (x, y) be any solution whatever. Then $215x - 611y = 215(54) - 611(19) = 1$; so

$$215(x - 54) = 611(y - 19). \tag{1}$$

This means that $611 \mid 215(x - 54)$. Since we have just shown that $\gcd(611, 215) = 1$, the Fundamental Theorem of Arithmetic tells us that $611 \mid (x - 54)$, i.e., that for some

$t \in \mathbb{Z}$, $x - 54 = 611t$, i.e., that $x = 54 + 611t$, as desired. Finally, plugging this into equation (1) gives $215(611t) = 611(y - 19)$, so that $215t = y - 19$ and $y = 19 + 215t$. Every solution therefore has the form we claimed.

- (b) The equation $52x - 143y = 1$ has no solutions, since the left hand side is a multiple of $13 = \gcd(52, 143)$, and the right hand side is not.

The equation $645x - 1833y = 3$ is equivalent (divide by 3) to $215x - 611y = 1$. We therefore found its solutions in part (a).

- (c) What do these problems have to do with the problems of finding $1/215$ in \mathbb{Z}_{611} and $1/52$ in \mathbb{Z}_{143} ? Well, $1/215$ exists in \mathbb{Z}_{611} iff there is a solution to the equation $215x = 1$ in \mathbb{Z}_{611} (and the solution x is the value of $1/215$). This happens iff there is a solution in \mathbb{Z} to $215x = 1 + 611y$, i.e., a solution to $215x - 611y = 1$. In other words, the value of $1/215$ is exactly the x -value of the solution in part (a). In \mathbb{Z}_{611} , $1/215 = 54$.

The same analysis shows that $1/52$ exists in \mathbb{Z}_{143} if and only if the equation $52x - 143y = 1$ has solutions in \mathbb{Z} , which it doesn't.

5. We are given that $a = bq + r$, and we want to show that

$$\gcd(a, b) = \gcd(b, r). \quad (2)$$

To prove equation (5), we prove that in fact the common divisors of a and b are the same as the common divisors of b and r .

So suppose that d is a common divisor of b and r . Then $d \mid bq$ and $d \mid r$; so $d \mid (bq + r)$. In other words, $d \mid a$; so d is a common divisor of a and b . Thus, every common divisor of b and r is a common divisor of a and b .

Conversely, suppose d is a common divisor of a and b . Then $d \mid bq$; so $d \mid (a - bq)$. In other words, $d \mid r$; so d is a common divisor of b and r .

Since the common divisors of a and b are the same as the common divisors of b and r , it follows at once that the greatest common divisor of a and b must be the greatest common divisor of b and r , i.e., that equation (2) is true.

This is one way to give an economical proof that Euclid's Algorithm works to compute gcds.

6. I'd start out and do the problem for primes and prime powers. If p is a prime, then

$$\begin{aligned} \nu(p^0) &= 1 \\ \nu(p^1) &= 1 \\ \nu(p^2) &= 2 \\ \nu(p^3) &= 2 \\ \nu(p^4) &= 3 \\ &\vdots \\ \nu(p^\alpha) &= 1 + \lfloor \alpha/2 \rfloor. \end{aligned}$$

Now let's look at what happens to a product of 2 prime powers. If p and q are distinct primes, then the squares dividing $p^\alpha q^\beta$ are exactly the products of the squares dividing p^α and the squares dividing q^β . That is,

$$\nu(p^\alpha q^\beta) = \nu(p^\alpha)\nu(q^\beta) = (1 + \lfloor \alpha/2 \rfloor)(1 + \lfloor \beta/2 \rfloor).$$

The obvious conjecture one would draw at this point is that

$$\nu(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = (1 + \lfloor \alpha_1/2 \rfloor)(1 + \lfloor \alpha_2/2 \rfloor) \cdots (1 + \lfloor \alpha_k/2 \rfloor)$$

It's possible to give an inductive proof of this claim, but I'd be OK with quitting here.