Math 300.1—Spring 2020
Solutions for Homework due April 23

1. Given positive integers $a$ and $b$, show that there exist integers $x$ and $y$ such that $\gcd(a, b) = xa + yb$. (Hint: Consider the set of integer linear combinations of $a$ and $b$ that are positive. The well-ordering principle says this set has a smallest element. Show that element is the gcd.)

The idea here is to give a proof that $\gcd(a, b)$ can be written as a linear combination of $a$ and $b$ without actually using the Euclidean Algorithm. This is Theorem 8.8, which the book says “Many mathematicians” prefer to prove using the Well-Ordering Principle.

Following the hint, let $X = \{ ax + by > 0 \mid x, y \in \mathbb{Z} \}$. This is a nonempty set of natural numbers, since, e.g., if $a \neq 0$ we can take $x = a$ and $y = 0$. (Note that we really need the hypothesis that not both $a$ and $b$ are 0, which I forgot to state in the problem.) So the Well-Ordering Principle says that $X$ has a smallest element. Let’s call that element $d$.

So we want to show that $d$ is $\gcd(a, b)$. First let’s show that $d$ is a common divisor of $a$ and $b$. According to the division theorem, there exist unique integers $q$ and $r$ such that $a = qd + r$ and $0 \leq r < d$. This gives $a - qd = r$, but $d = ax + by$ for some $x, y \in \mathbb{Z}$ since $d \in X$. So $r = a - qd = a - (ax + by) = a(1 - qx) - by$. If $r \neq 0$, this says it’s in $X$. But $r < d$ and $d$ is the smallest element in $X$. So $r$ can’t be in $X$ and therefore must be 0. That says $d \mid a$. Similarly, $d \mid b$.

To show $d$ is the greatest common divisor, let $c$ be any common divisor of $a$ and $b$. So $a = cj$ and $b = ck$ for some integers $j, k$. So $d = ax + by = c(jx + ky) = c(jx + ky)$, which says that $c \mid d$. So we must have $c \leq d$, showing that $d$ is really the greatest common divisor.

Section 8.1:

3. (a) Let $a \in \mathbb{Z}$ and let $k \in \mathbb{Z}$ with $k \neq 0$. Prove that if $k \mid a$ and $k \mid (a + 2)$, then $k \mid 2$.

If $k \mid a$ and $k \mid 2$ then we know that $k \mid (a + 2 - a)$. (Write $a + 2$ and $a$ as multiples of $k$ and subtract.) So $k \mid 2$.

(b) Let $a \in \mathbb{Z}$. What conclusions can be made about the greatest common divisor of $a$ and $a + 2$?

Part (a) shows that any common divisor of $a$ and $a + 2$ is a divisor of 2, so certainly $\gcd(a, a + 2)$ is a divisor of 2. The only positive divisors of 2 are 1 and 2, so we know $\gcd(a, a + 2)$ is 1 (if $a$ is odd) or 2 (if $a$ is even).
5. For each of the following pairs, use the Euclidean Algorithm to find \( \gcd(a, b) \) and to write \( \gcd(a, b) \) as a linear combination of \( a \) and \( b \). That is, find integers \( m \) and \( n \) such that \( d = am + bn \).

(c) \( a = 72, \ b = 714 \).

I’ll write out the arithmetic for this one, and just give the answers for the other two:

\[
714 = 72 \cdot 9 + 66 \\
66 = 6 \cdot 11 + 0.
\]

So \( \gcd(72, 714) = 6 \).

From the second equation, we have \( 6 = 72 - 66 \). The first equation says that \( 66 = 714 - 72 \cdot 9 \) substituting that into \( 6 = 72 - (714 - 72 \cdot 9) \) gives \( 6 = 72 - (714 - 72 \cdot 9) = 72 \cdot 10 + 714(-1) \).

(d) \( a = 12628, \ b = 21361 \)

The gcd is \( 41 = 12628 \cdot 181 + 21361 \cdot (-107) \)

(f) \( a = -36, \ b = -60 \)

For common factors, we can multiply either (or both) numbers by \(-1\) without changing the common factors. So we can do this with \( 36 \) and \( 60 \). The gcd is \( 12 \) and \( 12 = (-36)(-2) + (-60)(1) \).

Section 8.2:

7. (a) Let \( a = 16 \) and \( b = 28 \). Determine the value of \( d = \gcd(a, b) \) and then determine the value of \( \gcd(\frac{a}{d}, \frac{b}{d}) \).

\[
\gcd(16, 28) = 4 \quad \text{and} \quad \gcd(4, 7) = 1.
\]

(b) Repeat Exercise (7a) with \( a = 10 \) and \( b = 45 \).

\[
\gcd(10, 45) = 5 \quad \text{and} \quad \gcd(2, 9) = 1.
\]

(c) Let \( a, b \in \mathbb{Z}, \) not both equal to \( 0, \) and let \( d = \gcd(a, b) \). Explain why \( \frac{a}{d} \) and \( \frac{b}{d} \) are integers. Then prove that \( \gcd(\frac{a}{d}, \frac{b}{d}) = 1 \).

We know that \( d \) is a factor of both \( a \) and \( b, \) so \( \frac{a}{d} \) and \( \frac{b}{d} \) are integers.

Since \( d = \gcd(a, b), \) we know that there are integers \( x, y \) such that \( xa + yb = d \). Dividing this equation by \( d \) gives \( x\frac{a}{d} + y\frac{b}{d} = 1, \) showing that \( \gcd(\frac{a}{d}, \frac{b}{d}) = 1 \).

8. Are the following propositions true or false? Justify your conclusions.

(a) For all integers \( a, \ b, \) and \( c, \) if \( a \mid c \) and \( b \mid c, \) then \( (ab) \mid c. \)

This is false. A counterexample is \( a = 4, \ b = 6 \) and \( c = 12. \)
(b) For all integers \(a, b, \) and \(c\), if \(a \mid c\), \(b \mid c\), and \(\gcd(a, b) = 1\), then \((ab) \mid c\).

This proposition is true. To see that, take \(a, b, c\) with \(a \mid c\), \(b \mid c\) and \(\gcd(a, b) = 1\). So there exist \(m, n \in \mathbb{Z}\) with \(ma = c\) and \(nb = c\), and there exist \(x, y \in \mathbb{Z}\) with \(xa + yb = 1\). Then \(cxa + cyb = c\). If we substitute \(nb\) for the \(c\) in \(cxa\) and \(ma\) for the \(c\) in \(cyb\), we get

\[
abnx + abmy = c.
\]

It’s clear that \(ab\) divides the left side, so \((ab) \mid c\).

10. (a) Prove the following proposition: For all \(a, b, c \in \mathbb{Z}\), \(\gcd(a, bc) = 1\) if and only \(\gcd(a, b) = 1\) and \(\gcd(a, c) = 1\).

There are a couple of ways you could do this.

One is to observe that, if \(\gcd(a, b) = 1 = \gcd(a, c)\), there exist integers \(m, n, x, y\) such that \(am + bn = 1\) and \(ax + cy = 1\). So we have

\[
1 = (am + bn)(ax + cy) = a^2mx + amcy + abnx + bcny = a(2mx + cny) + (bc)(ny).
\]

This proves that \(\gcd(a, bc) = 1\). For the converse, if \(\gcd(a, bc) = 1\), there exist integers \(s, t\) such that \(as + (bc)t = 1\). So \(ax + b(ct) = 1\), showing that \(\gcd(a, b) = 1\) and \(ax + c(bt) = 1\), showing that \(\gcd(a, c) = 1\).

Another way is to use the Fundamental Theorem of Arithmetic. To say that the gcd of two numbers is 1 is, by the Fundamental Theorem and the definition of gcd, the same as saying that there is no prime number that divides both of the numbers. The Fundamental Theorem implies that the set of primes that divide the product \(bd\) is the union of the set of primes dividing \(b\) and the set of primes dividing \(c\). So there’s no prime that divides both \(a\) and \(bc\) if and only if there is no prime that divides both \(a\) and \(b\) or both \(a\) and \(c\).

(b) Use mathematical induction to prove the following proposition: Let \(n \in \mathbb{N}\) and let \(a, b_1, b_2, \ldots, b_n \in \mathbb{Z}\). If \(\gcd(a, b_i) = 1\) for all \(i \in \mathbb{N}\) with \(i \leq n\), then \(\gcd(a, b_1, \ldots, b_n) = 1\).

Let \(P(n)\) be the statement that, if \(\gcd(a, b_1) = 1\) for \(i = 1, \ldots, n\), then \(\gcd(a, b_1b_2 \ldots b_n) = 1\). It’s clear that \(P(1)\) is true, and part (a) shows that \(P(2)\) is true. Let \(k \in \mathbb{N}\). We prove that \(P(k) \rightarrow P(k + 1)\).

So assume \(P(k)\) is true and let \(b_1, \ldots, b_{k+1}\) be integers such that \(\gcd(a, b_i) = 1\) for \(i = 1, \ldots, k + 1\). Let \(b = \)
b_1 b_2 \ldots b_k. By the induction hypothesis that \( P(k) \) is true, we know that \( \gcd(a, b) = \gcd(a, b_1 b_2 \ldots b_k) = 1 \). But then part (a) says that \( \gcd(a, b b_{k+1}) = 1 \). Since \( b b_{k+1} = b_1 b_2 \ldots b_{k+1} \), this completes the proof.

17. Prove the following proposition: Let \( n \in \mathbb{N} \). For each \( a \in \mathbb{Z} \), if \( \gcd(a, n) = 1 \), then for every \( b \in \mathbb{Z} \), there exists an \( x \in \mathbb{Z} \) such that \( ax \equiv b \pmod{n} \).

(Hint: One way is to start by writing 1 as a linear combination of \( a \) and \( n \).

If \( \gcd(a, n) = 1 \), then there exist \( s, t \in \mathbb{Z} \) with \( as + nt = 1 \). So \( as \equiv 1 \pmod{n} \). It follows that \( abs \equiv b \pmod{n} \). Taking \( x = bs \) gives \( ax \equiv b \pmod{n} \).

Section 8.3:

3. Determine all solutions to the following linear Diophantine equations:

(f) \( 200x + 54y = 21 \)

There is no solution. 2 is a common factor of 54 and 200, so 2 must divide the gcd of 54 and 200. But 2 does not divide 21, so \( \gcd(200, 54) \) doesn’t divide 21.

(h) \( 12x + 18y = 6 \)

We have \( \gcd(12, 18) = 6 \), so there are solutions, the most obvious one of which is \((−1)/(12) + (1)/(18) = 6 \). So all solutions have the form \( x = −1 + \frac{18}{6}k \) and \( y = 1 − \frac{12}{6}k \).

9. The purpose of this exercise will be to prove that the nonlinear Diophantine equation \( 3x^2 − y^2 = −2 \) has no solution.

(a) Explain why if there is a solution of the Diophantine equation \( 3x^2 − y^2 = −2 \), then that solution must also be a solution of the congruence \( 3x^2 − y^2 \equiv −2 \pmod{3} \).

If \( 3x^2 − y^2 \) is equal to \( −2 \), it’s certainly congruent to \( −2 \) modulo 3. (Or modulo any other \( n \), for that matter.)

(b) If there is a solution of the Diophantine equation \( 3x^2 − y^2 = −2 \), explain why there then must be an integer \( y \) such that \( y^2 \equiv 2 \pmod{3} \).

For any \( x \), \( 3x^2 \equiv 0 \pmod{3} \). So our congruence from part (a) says \( −y \equiv −2 \pmod{3} \). But that’s equivalent to \( y \equiv 2 \pmod{3} \).

(c) Use a proof by contradiction to prove that the Diophantine equation \( 3x^2 − y^2 = −2 \) has no solution.

If there is a solution to the given Diophantine equation, there must be an integer \( y \) whose square is congruent to 2, modulo 3. But in \( \mathbb{Z}_3 \), \([1]^2 = [1] \) and \([2]^2 = [1] \), while
\[0]^2 = [0] \text{ as always. So there is no integer } y \text{ with } y^2 \equiv 2 \pmod{3}, \text{ and thus no solutions to the Diophantine equation } 3x^2 - y^2 = -2.\]