

1. (a) Prove that  $\gcd(m, 0) = m$  for all integers  $m > 0$ .

Clearly  $m$  is a common divisor of  $m$  and  $0$ .

By a Lemma in class, if  $d|m$ , then  $d \leq m$ .

Thus every common divisor of  $m$  and  $0$  is less than or equal to  $m$ . Hence  $m = \gcd(m, 0)$

- (b) Prove that  $\gcd(m, n) = \gcd(n, m \bmod n)$  for all positive integers  $m$  and  $n$ .

Let  $r = m \bmod n$ . Then there exists  $q \in \mathbb{Z}$  such that  $m = qn + r$ . If  $d_1$  divides both  $m$  and  $n$ , then  $d_1$  divides  $m - qn = r$ . Also, if  $d_2$  divides both  $n$  and  $r$ , then  $d_2$  divides  $qn + r = m$ . Hence the set of common divisors of  $m$  and  $n$  is equal to the set of common divisors of  $n$  and  $r$ . Thus  $\gcd(m, n) = \gcd(n, r)$ .

- (c) Which important theorem, proved in class, do the above facts help to prove?

The Euclidean Algorithm.

2. (a) State the Division Algorithm.

Let  $m, n \in \mathbb{Z}$  with  $n > 0$ . Then there exists unique integers  $q \in \mathbb{Z}$  and  $0 \leq r < n$  such that

$$m = qn + r.$$

(b) Show that an integer  $n$  is not even if and only if there exists an integer  $k$  such that  $n = 2k + 1$ .

Suppose that  $n$  is not even. By the Division Algorithm there exists  $q \in \mathbb{Z}$  and  $0 \leq r < 2$  such that  $n = 2q + r$ . Since  $n$  is not even, we must have  $r = 1$ . Suppose  $\exists k \in \mathbb{Z}$  such that  $n = 2k + 1$ . If  $n$  were even, then there would exist  $m \in \mathbb{Z}$  such that  $n = 2m + 0$ . But this cannot be so, since it would contradict the Division Algorithm.

(c) Suppose that there exists an integer  $k$  such that  $n = 12k + 5$ . Must it be true that  $\gcd(n, 12) = 1$ ?

Yes. For we see that  $5 = n \pmod{12}$ . Hence

$$\begin{aligned} \gcd(n, 12) &= \gcd(12, n \pmod{12}) \\ &= \gcd(12, 5) = 1. \end{aligned}$$

3. (a) Find all solutions (if any) of the linear system

$$\begin{cases} x \equiv 44 \pmod{105} \\ x \equiv 17 \pmod{81}. \end{cases}$$

We look for a solution  $x \in \mathbb{Z}$  of the form

$$x = 44 + 105t, \quad t \in \mathbb{Z}.$$

Plug this into the second congruence and solve for  $t$ :

$$105t \equiv -27 \pmod{81}.$$

Perform the Euclidean Algorithm:

$$1 \cdot 105 + 0 \cdot 81 = 105$$

$$0 \cdot 105 + 1 \cdot 81 = 81$$

$$1 \cdot 105 + (-1) \cdot 81 = 24$$

$$(-3) \cdot 105 + 4 \cdot 81 = 9$$

$$7 \cdot 105 + (-9) \cdot 81 = 6$$

$$\boxed{(-10) \cdot 105 + 13 \cdot 81 = 3} \rightarrow \gcd(105, 81) = 3$$

Thus if we multiply by  $-9$ , we get

$$105 \cdot 90 = 3 + (9 \cdot 13) \cdot 81, \quad \text{so } 105 \cdot 90 \equiv 3 \pmod{81}.$$

Plug  $t=90$  into our guess for  $x$  to get  $x = 44 + 105 \cdot 90 = 9494$ .

$$\text{Since } 81 \cdot 105 / \gcd(81, 105) = \frac{81 \cdot 105}{3} = 2835,$$

we see that the set of solutions of our linear system is

$$\{x \in \mathbb{Z} \mid x \equiv 9494 \pmod{2835}\}.$$

4. (a) Prove or provide a counterexample: For all positive integers  $m$  and  $n$ ,

$$\gcd(m + 2n, 3n) = \gcd(m, n).$$

Take  $m = n = 3$  to get

$$\gcd(m + 2n, 3n) = \gcd(9, 9) = 9,$$

but  $\gcd(m, n) = \gcd(3, 3) = 3.$

(b) Prove or provide a counterexample: If  $\gcd(a, b) = 1$ , then  $\gcd(b, c) = 1$  if and only if  $\gcd(a, c) = 1$ .

This is false. Take  $a = 5$ ,  $b = 3$ ,  $c = 10$ . Then

$$\gcd(a, b) = \gcd(5, 3) = 1,$$

$$\gcd(b, c) = \gcd(3, 10) = 1,$$

but  $\gcd(a, c) = \gcd(5, 10) = 5.$

5. (Bonus)

(a) Let  $a_n$  be the sequence recursively defined by

$$\begin{cases} a_1 = 2 \\ a_{k+1} = a_k^2 - a_k + 1 \quad (k \geq 1) \end{cases}$$

Show that  $a_n = 1 + \prod_{j=1}^{n-1} a_j$  for every  $n \geq 2$ .

Since  $a_2 = a_1^2 - a_1 + 1 = 3 = 1 + 2$ , the formula holds for  $n=2$ .

Suppose the formula holds for  $n=k$ :  $a_k = 1 + \prod_{j=1}^{k-1} a_j$ .

$$\text{Then } a_{k+1} = \left(1 + \prod_{j=1}^{k-1} a_j\right) \cdot a_k - \cancel{a_k} + 1$$

$$= a_k + \prod_{j=1}^{k-1} a_j \cdot a_k - \cancel{a_k} + 1 = 1 + \prod_{j=1}^k a_j.$$

The result now follows by induction.

(b) Show that  $\gcd(a_n, a_m) = 1$  for all positive integers  $m$  and  $n$  such that  $m \neq n$ .

Without loss of generality, suppose  $1 \leq n < m$ . Then

$$\gcd(a_m, a_n) = \gcd(a_n, a_m \bmod a_n).$$

The proof will be complete once we show that  $a_m \bmod a_n = 1$ .

But this is easy:

$$a_m = \left[ \prod_{\substack{j=1 \\ j \neq n}}^{m-1} a_j \right] \cdot a_n + 1.$$