Worksheet 8: Euclidean Algorithm, Enumerating Primes, Review

Problem 1. Compute the following gcds using the Euclidean algorithm. Then work backwards through the Euclidean algorithm to express this gcd as a linear combination of the two numbers.

(a) $\gcd(105, 27)$ (b) $\gcd(1479, 272)$

Solution. We divide repeatedly:

$$\begin{aligned} 105 &= 3 \cdot 27 + 24 \\ 27 &= 1 \cdot 24 + 3 \\ 24 &= 6 \cdot 3 + 0 \end{aligned}$$

Since the last nonzero remainder is 3, this is the gcd. We then work backwards:

$$3 = 27 - 1 \cdot 24 = 27 - 1 \cdot (105 - 3 \cdot 27) = 4 \cdot 27 - 1 \cdot 105.$$

Now the same thing for (b).

$$\begin{aligned} 1479 &= 5 \cdot 272 + 119 \\ 272 &= 2 \cdot 119 + 34 \\ 119 &= 3 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}$$

Thus 17 is the gcd and

$$\begin{aligned} 17 &= 119 - 3 \cdot 34 \\ &= 119 - 3 \cdot (272 - 2 \cdot 119) = 7 \cdot 119 - 3 \cdot 272 \\ &= 7 \cdot (1479 - 5 \cdot 272) - 3 \cdot 272 = 7 \cdot 1479 - 38 \cdot 272 \end{aligned}$$

Problem 2. How many prime numbers are less than 121?

Solution. Any composite number less than 121 must have a prime factor that's less than $\sqrt{121} = 11$, so it must have a prime factor of 2, 3, 5 or 7. We thus go through the list of numbers from 1 to 100, crossing out 1 and all nontrivial multiples of 2, 3, 5, and 7, and 11. What remains will be the primes. Once one does this (omitted), one finds 30 primes.

Problem 3. Show that $\gcd(21n + 4, 14n + 3) = 1$ for all positive integers n.

Solution. We use the euclidean algorithm:

$$\begin{aligned} 21n + 4 &= 1 \cdot (14n + 3) + (7n + 1) \\ 14n + 3 &= 2 \cdot (7n + 1) + 1 \\ 7n + 1 &= (7n + 1) \cdot 1 + 0 \end{aligned}$$

Since 1 is the last nonzero remainder, this is the gcd.

Problem 4. Prove that there exist no integers x and y such that $1691x + 1349y = 1$.

Solution. We use the Euclidean algorithm to compute $\gcd(1691, 1349) = 19$ (omitted). Since the gcd is the smallest positive linear combination of 1691 and 1349 by Bézout's theorem, we know that 1 cannot be a linear combination.

Problem 5. Prove that, for any integer $n \geqslant 2$ and any collection of sets $A_1, \dots, A_n$ inside some universal set, we have

$$\overline{A_1 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}.$$

Solution. First we prove the base case $n = 2$. Let A_1 and A_2 be two sets. Then $x \in \overline{A_1 \cup A_2}$ iff $x \notin A_1 \cup A_2$ iff $x \notin A_1$ and $x \notin A_2$ iff $x \in \overline{A_1} \cap \overline{A_2}$. Thus $\overline{A_1 \cup A_2} = \overline{A_1} \cap \overline{A_2}$.

Now suppose the statement is true for $n = k$. Let $A_1, \dots, A_{k+1}$ be sets inside some universal set. Then

$$\begin{aligned} \overline{A_1 \cup \cdots \cup A_k \cup A_{k+1}} &= \overline{(A_1 \cup \cdots \cup A_k) \cup A_{k+1}} \\ &= \overline{A_1 \cup \cdots \cup A_k} \cap \overline{A_{k+1}} \\ &= (\overline{A_1} \cap \cdots \cap \overline{A_k}) \cap \overline{A_{k+1}} \\ &= \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_{k+1}} \end{aligned}$$

where we use the base case of our induction for the second equality, and the inductive hypothesis for the third equality. This completes the induction.

Problem 6. Suppose n is a positive integer. If a is an integer, an integer b is called an *inverse of* a *modulo* n if $ab \equiv 1 \bmod n$.

(a) Show that 3 has an inverse modulo 17.

(b) Show that 3 does *not* have an inverse modulo 18.

Solution. For part (a), we're looking for an integer b such that $3b \equiv 1 \bmod 17$, ie, $3b - 1 = 17x$ for some x, or $3b - 17x = 1$. In other words, we just need to write 1 as a linear combination of 17 and 3 and we'll be done. We can do this using the Euclidean algorithm:

$$17 = 5 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

Thus

$$1 = 3 - 2 = 3 - (17 - 5 \cdot 3) = 6 \cdot 3 - 17.$$

For part (b), an inverse of 3 modulo 18 would be an integer b such that $3b - 1 = 18x$, ie, $3b - 18x = 1$. But $\gcd(3, 18) = 3$, so by Bézout's theorem, 1 cannot be a linear combination of 3 and 18.

Problem 7. Prove that if $a \mid n$ and $b \mid n$ with $\gcd(a, b) = 1$, then $ab \mid n$ using...

(a) Bézout's theorem.

(b) Ste17, Lemma 1.1.17.

Solution. The key observation, for both proofs, is that $a \mid n$ implies $ab \mid bn$ and that $b \mid n$ implies $ab \mid an$. In other words, ab divides both an and bn.

(a) By Bézout's theorem, there exist integers x, y such that $ax + by = 1$. Then

$$anx + bny = n.$$

By what we noted above, ab divides the left-hand side of the above equation, so it must also divide n.

(b) By Ste17, lemma 1.1.17, we have

$$\gcd(an, bn) = \gcd(a, b) \cdot |n| = |n|.$$

Since ab divides both an and bn, we have $ab \mid \gcd(an, bn)$, which in turn divides $|n|$, which divides n. Thus $ab \mid n$.

Problem 8. Do there exist integers x and y such that $172x + 20y = 1000$? Justify.

Solution. Yes there do. We find that $\gcd(172, 20) = 4$ and that

$$4 = 2 \cdot 172 + (-17) \cdot 20.$$

Multiplying through by 250, we get

$$1000 = 500 \cdot 172 + (-4250) \cdot 20.$$

Thus we can take $x = 500$ and $y = -4250$.

Problem 9. Suppose $\gcd(a, b) = 1$. Is it true that $\gcd(ab, a + b) = 1$? Justify.

Solution. It is true. We prove this by contraposition. Suppose $\gcd(ab, a + b) \neq 1$. Then there exists a prime p dividing $\gcd(ab, a + b)$, so it in particular divides ab. But then it divides either a or b by Euclid's lemma. Since p also divides $a + b$, it must divide both a and b. Thus $p \mid \gcd(a, b)$, so $\gcd(a, b) \neq 1$.

Problem 10. Consider the real number

$$\alpha = 0.235711131719 \cdots,$$

whose digits after the decimal point are obtained by stringing together the decimal representations of all of the primes. Show that α is irrational. *Hint*. Use contradiction. You may use the fact that a number whose decimal expansion never repeats is irrational (ie, the converse of a problem from a previous worksheet, which we have not proved yet). You might decide to use Dirichlet's theorem on arithmetic progressions (Ste17, theorem 1.2.7) by considering the progression $10^{n+1}x + 1$ for some appropriate choice of n.

Solution. Suppose for a contradiction that α is rational. For every positive integer i, let $a_i \in \{0, 1, ...9\}$ denote the ith digit of α after the decimal point. Since α is rational, there exists integers $m \geqslant 0$ and $k > 0$ such that $a_i = a_{i+k}$ for all $i > m$. Since the set of prime numbers is infinite, the repeating digits $a_{m+1}, \ldots, a_{m+k}$ cannot all be 0 (if they were all 0, then α would have the finite decimal expansion $0.a_1 a_2 \cdots a_m$).

Fix any positive integer $n > m + k$. By Dirichlet's theorem, there exists a prime p of the form $10^{n+1}x + 1$ (in fact, there exist infinitely many such primes, but we won't need this). This means that the decimal representation of p ends with

$$\cdots \underbrace{0 \cdots 0}_{n \text{ times}} 1.$$

Let $r \geqslant 1$ be the integer marking the position in α just before the first of n zeroes of p. In other words, $a_{r+1}, \ldots, a_{r+n}$ are all 0. In particular, the k digits $a_{r+m+1}, \ldots, a_{r+m+k}$ are all 0. But $r + m + 1 \geqslant m + 1$, so the k repeating digits $a_{m+1}, \ldots, a_{m+k}$ all occur among $a_{r+m+1}, \ldots, a_{r+m+k}$. This implies that all of the repeating digits must be 0, but this contradicts our observation that the repeating digits are not all 0.