1 Solutions to assignment 3, due May 31

Problem 11.26 Use the Euclidean Algorithm to find the GCD for each of the following pairs of integers:

Solution: (a) 51 and 288

In this case, we write $288 = 5 \cdot 51 + 33$. Following through, we obtain

$$\begin{aligned} 51 &= 1 \cdot 33 + 18 \\ 33 &= 1 \cdot 18 + 15 \\ 18 &= 1 \cdot 15 + 3 \\ 15 &= 5 \cdot 3 \end{aligned}$$

and therefore $gcd(288, 51) = 3$.

(b) 357 and 629

In this case, we have again

$$\begin{aligned} 629 &= 1 \cdot 357 + 272 \\ 357 &= 1 \cdot 272 + 85 \\ 272 &= 3 \cdot 85 + 17 \\ 85 &= 5 \cdot 17 \end{aligned}$$

and so $gcd(629, 357) = 17$.

(c) 180 and 252

Lastly, we have

$$\begin{aligned} 252 &= 1 \cdot 180 + 72 \\ 180 &= 2 \cdot 72 + 36 \\ 72 &= 2 \cdot 36 \end{aligned}$$

which yields that $gcd(252, 180) = 36$.

Problem 11.27 Determine integers x, y such that

Solution: (a) $gcd(51, 288) = 51x + 288y$.

We work backwards:

$$\begin{aligned} 3 &= 18 - 1 \cdot 15 \\ &= 18 - 1 \cdot (33 - 1 \cdot 18) = 2 \cdot 18 - 1 \cdot 33 \\ &= 2 \cdot (51 - 1 \cdot 33) - 1 \cdot 33 = 2 \cdot 51 - 3 \cdot 33 \\ &= 2 \cdot 51 - 3 \cdot (288 - 5 \cdot 51) = 17 \cdot 51 - 3 \cdot 288 \end{aligned}$$

(b) $gcd(357, 629) = 357x + 629y$.
In this case, we have again

$$\begin{aligned}17 &= 272 - 3 \cdot 85 \\ &= 272 - 3 \cdot (357 - 1 \cdot 272) = 4 \cdot 272 - 3 \cdot 357 \\ &= 4 \cdot (629 - 1 \cdot 357) - 3 \cdot 357 = 4 \cdot 629 - 7 \cdot 357\end{aligned}$$

(c) $gcd(180, 252) = 180x + 252y$.
Lastly, we have

$$\begin{aligned}36 &= 180 - 2 \cdot 72 \\ &= 180 - 2 \cdot (252 - 1 \cdot 180) \\ &= 3 \cdot 180 - 2 \cdot 252\end{aligned}$$

Problem 11.28 Let a and b be integers, not both 0. Show that there are infinitely many pairs s, t of integers such that $gcd(a, b) = as + bt$.

Solution: We first show, as per the hint, that there are infinitely many integers m, n such that $ma + nb = 0$. We note of course that if $n = -a$ and $m = b$, that $ma + nb = ba - ab = 0$. Thus we see that, for any $k \in \mathbb{Z}$, the integers $m = kb$ and $n = -ka$ have the desire property; there are infinitely many of these.

If we then add the two equations

$$1 = as + bt \qquad\qquad 0 = (kb)a + (-ka)b$$

together, we find that

$$1 = (s + kb)a + (t - ka)b$$

is true for any $k \in \mathbb{Z}$ as desired.

Problem 11.34 Use Corollary 11.14 to prove that $\sqrt{3}$ is irrational.

Solution: Corollary 11.14 states that if p is prime, and $p \mid ab$, then $p \mid a$ or $p \mid b$.

So assume that $\sqrt{3}$ is rational, i.e. $\sqrt{3} = \frac{p}{q}$ for relatively prime integers p, q. In particular, at most one of them is divisible by 3.

This is equivalent to $3q^2 = p^2$. This of course implies that $3 \mid p^2$. Using the corollary, we see that either $3 \mid p$ or $3 \mid p$... i.e. we conclude that $3 \mid p$. We then conclude that, as q, p have no common factors, that $3 \nmid q$.

Writing $p = 3k$ for some integer k we find that we have $3q^2 = (3k)^2 = 9k^2$. Cancelling a factor of 3 we obtain $q^2 = 3k^2$. However, we can now conclude that $3 \mid q^2$ and thus, using the corollary again, that $3 \mid q$. But this contradicts that p, q have no common factors.

Q.E.D.

Problem 11.36 Let p be a prime, and let $n \in \mathbb{Z}$ with $n \geq 2$. Prove that $p^{1/n}$ is irrational.

Solution: There are two likely proofs of this. The first is as follows.

Suppose that $p^{1/n} = a/b$ for integers a, b with no common factors. Then this is equivalent to $b^n p = a^n$.

Using the same corollary as before, we see that $p \mid a^n$, and thus we can conclude that $p \mid a$. But this means that we can write $a = pk$ for some integer k, and so

$$b^n p = (pk)^n = p^n k^n$$

or, upon simplifying, $b^n = p \cdot p^{n-2} k^n$.

Hoewver, this implies that $p \mid b^n$ which implies yet again that $p \mid b$! As we assumed that a, b had no common factors, we have found our desired contradiction.

Q.E.D.

The other proof involves looking at the prime factorizations of a and b; all exponents on the right-hand side are multiples of n, but at least one on the left hand side (that of p) has remainder 1 when dividing by n, which is a contradiction.

Problem 11.37 Prove that if $p \geq 2$ is an integer witht he property that for every pair a, b of integers, $p \mid ab$ implies that $p \mid a$ or $p \mid b$, then p is prime.

Solution: We look at the contrapositive form of this statement. That is, we prove instead that

If p is composite, then there exist integers a, b such that $p \mid ab$, but $p \nmid a$ and $p \nmid b$.

We need to exhibit an example of such integers a, b, given composite p.

If p is composite, then $p = xy$ for some integers $x, y \geq 2$. So choose $x = a$ and $y = b$. Then as $p = ab$, we clearly have that $p \mid ab$. However, as $a, b < p$, we cannot have that $p \mid a$ or $p \mid b$!

Thus we have proven the contrapositive, and we are done.

Q.E.D.

Problem 11.38a Prove that every two consecutive odd positive integers are relatively prime.

Solution: Let $2n-1$ and $2n+1$ be our two consecutive odd positive integers, and let $d \mid 2n-1$, $d \mid 2n+1$.

As $d \mid a$ and $d \mid b$ implies that $d \mid (a \pm b)$, we have in this case that

$$d \mid (2n+1) - (2n-1) = 2$$

Thus $d = 1$ or $d = 2$. If $d = 2$, then $2 \mid (2n+1)$. But this is clearly false, and so the only possibility is that $d = 1$. Thus the only divisor of $2n-1$ and $2n+1$ is 1, and so they are relatively prime as claimed.

Q.E.D.