MA357, Spring 2020 — Problem Set 2 Solutions

1. NTG, Exercise 2.11.18.

There is a trick; here's how you might come up with it. Let a and b be integers with $b > a$. Then $b^2 - a^2$ always factors:

$$b^2 - a^2 = (b - a)(b + a).$$

We want to show that every odd number can be written in this way. That seems unlikely, since some odd integers are primes! Thinking this through, one realizes that if $n = b^2 - a^2$ is going to be equal to a prime, then $b - a = 1$, so $b = a + 1$. But then $n = a + b = 2b + 1$, and any odd number looks like $2b + 1$ for some b. That reveals the trick: if $n = 2b + 1$ then $n = (b + 1)^2 - b^2$.

Notice that this also gives a proof that

$$1 + 3 + 5 + \cdots + 2b + 1 = (b + 1)^2.$$

(Just use induction on b.)

2. Find the gcd of 771769 and 32378, and express it as a linear combination of these two numbers.

This one is basically just work: follow the algorithm (or, more likely, use Sage's `xgcd` command), and it comes out. We get that $\gcd(771769, 32378) = 1$, and taking $x = -14281, y = 340405$ makes $771769x + 32378y = 1$ (another solution is $x = 18097, y = -431364$).

3. Suppose you know that $\gcd(a, b) = 1$. What can you say about each of the following?

a. $\gcd(a + b, a - b)$

If $d|(a + b)$ and $d|(a - b)$ then, taking the sum and difference, we see that $d|(2a)$ and $d|(2b)$. So consider two cases:

- If d is even, say $d = 2u$. Then it follows that $u|a$ and $u|b$, hence, given our assumption, that $u = 1$ (or -1, but gcds are positive). Hence, $d = 2$.

- If d is odd, then $\gcd(d, 2) = 1$, and we can conclude that $d|a$ and $d|b$, and hence that $d = 1$.

So the $\gcd$ is either 1 or 2. Both cases can occur (consider $a = 2, b = 3$ and $a = 3, b = 5$).

Can we do it using linear combinations? Well, we're given that $\gcd(a, b) = 1$, so we know we can find r and s such that $ar + bs = 1$. Suppose we try to find x and y such that $(a+b)x+(a-b)y = 1$. This equation turns into $a(x+y) + b(x-y) = 1$, so we want $x + y = r, x - y = s$, which works out to $x = (r + s)/2$ and $y = (r - s)/2$. If r and s are both odd, we can do that, and we get $\gcd(a + b, a - b) = 1$. Otherwise, taking $x = r + s$ and $y = r - s$ gives $(a + b)x + (a - b)y = 2$, and the $\gcd$ is either 1 or 2.

b. $\gcd(a, a + b)$

If $d|a$ and $d|(a + b)$, then $d|b$, so $d = 1$. So $\gcd(a, a + b) = 1$.

Alternatively, given $ar + bs = 1$, we have $a(r - s) + (a + b)s = 1$.

c. $\gcd(2a, 2b)$

Clearly 2 is a common divisor. To show that it is the greatest common divisor, argue as in (a): any odd common divisor must be either 1 or -1, and any even common divisor must be either 2 or -2. So the gcd is 2.

Linear combinations work too: from $ax+by = 1$, we get $(2a)x+(2b)y = 2$, and it follows that the $\gcd$ is either 1 or 2. Since 2 clearly *is* a common divisor, it must be the $\gcd$.

d. $\gcd(2a, b)$

Again, either 1 or 2, depending on whether b is even or not.

4. Let $n \geqslant 1$ be an integer. Prove that $n! + 1$ and $(n + 1)! + 1$ are always relatively prime.

Remember that $(n + 1)! = (n + 1)n!$. So if we let $a = n! + 1$ and $b = (n + 1)! + 1$, then $(n + 1)a - b = n$. So if r divides a and b, we can conclude that r also divides $n>$ But if r divides n, it divides $n!$. So r divides both $n!$ and $n!+1$, hence divides their difference, which is 1. Hence $r=1$.

It's probably possible to find an explicit linear combination that's equal to 1, but it's hardly worth the effort.

5. In 1509, DeBouvelles claimed that for every $n \geqslant 1$ at least one of the numbers $6n-1$ and $6n+1$ was prime. Find a counterexample to show that he was wrong, then show that there are infinitely many counterexamples (i.e., show that there are infinitely many n such that both $6n-1$ and $6n+1$ are composite).

Finding counterexamples is easy: in Sage,

```
for i in range (1,39):
    print '%6s %9s %9s'%(i,factor(6*i-1),factor(6*i+1))
```

Yields

```
     1         5         7
     2        11        13
     3        17        19
     4        23       5^2
     5        29        31
     6     5 * 7        37
     7        41        43
     8        47       7^2
     9        53    5 * 11
    10        59        61
    11    5 * 13        67
    12        71        73
    13    7 * 11        79
    14        83    5 * 17
    15        89    7 * 13
    16    5 * 19        97
    17       101       103
    18       107       109
    19       113    5 * 23
    20    7 * 17      11^2
```

He is not only dull himself, he is the cause of dullness in others.

```
21        5^3         127
22        131      7 * 19
23        137         139
24    11 * 13      5 * 29
25        149         151
26     5 * 31         157
27     7 * 23         163
28        167        13^2
29        173     5^2 * 7
30        179         181
31     5 * 37     11 * 17
32        191         193
33        197         199
34     7 * 29      5 * 41
35    11 * 19         211
36     5 * 43      7 * 31
37    13 * 17         223
38        227         229
```

Looking at the list confirms that the assertion is false, though the first counterexample happens only when $k = 20$. The other thing we see is that the counterexamples aren't all that frequent at first, so we need to be smart to prove that there are infinitely many of them.

The proof I like is based on the idea that it's easier to prove what we want if we replace "is composite" by something more specific. For example, suppose we want to find n such that $6n-1$ is divisible by 5, and $6n+1$ is divisible by 7. Of course $n = 1$ works, because we get exactly 5 and 7. If we can find larger ns that do this, then both $6n-1$ and $6n+1$ will have to be composite.

To do that, the key is to note that if we add 5 to n we don't change the fact that $6n-1$ is divisible by 5. Similarly for adding 7. So let's use the fact that adding 5 seven times is the same as adding 7 five times, i.e., let's add $35 = 5 \times 7$. The difference between $6(n+35)-1$ and $6n-1$ is divisible by 5, and the difference between $6(n+35)+1$ and $6n+1$ is divisible by 7. (Both differences are equal to $6 \times 35 = 210$, of course.) It follows that for any integer x if we take $n = 1+35x$ we will have $6n-1$ divisible by 5 and $6n+1$ divisible by 7, and so (except when $x = 0$) neither will be prime. (This is basically a congruence argument: we are "pasting together" a congruence $\pmod 5$ and a congruence $\pmod 7$ to get a congruence $\pmod{35}$.)

The number you have dialed is imaginary. Rotate phone 90 degrees and try again.

One can do the same thing by taking $n = 2 + 143x$, for example. This time the crucial divisors are 11 and 13. The apparent rarity of counterexamples is just a consequence of the fact that these sequences have long(ish) periods. For large n, it's more likely than not that neither $6n - 1$ nor $6n + 1$ will be prime. On the other hand, it seems likely that every so often one of them will indeed be prime. Are there infinitely many values of n for which one of the two expressions gives a prime?

6. One egg timer can time an interval of exactly 5 minutes, and a second can time an interval of exactly 11 minutes. How can we boil an egg for exactly 3 minutes (without buying another timer)?

This boils down (!) to solving the equation $5x + 11y = 3$. Taking $x = 5$ and $y = -2$ works, as does taking $x = -6$ and $y = 3$. Both solutions can easily be translated into little stories about egg timers.

7. NTG, Exercise 2.11.23.

First we compute $\gcd(203, 119) = 7$. So the three equations in part (a) have no integer solutions. For part (b), note first that $(-7) \times 119 + (12) \times 203 = 7$ (which I found using Sage). So the base solution is $x_0 = -49$, $y_0 = 84$. Since $203/7 = 29$ and $119/7 = 17$, the general solution is $x = -49 + 17k$, $y = 84 - 29k$. The solution closest to $(0, 0)$ happens when $k = 3$: $x = 2, y = -3$.

8. Find all the integer solutions of $15x + 7y = 310$, and then decide how many of them are *positive* integer solutions.

We first need to solve $15r+7s = 1$, which, fortunately, is easy: $r = 1, s = -2$. Now we just scale everything by 310. Hence a first solution is $x = 310, y = -620$. The general solution then is

$$\begin{aligned} x &= 310 - 7k \\ y &= -620 + 15k \end{aligned}$$

and the issue now is to find k so that both are positive. From $310 - 7k > 0$, we get $k < 44.2$, and from $-620 + 15k > 0$ we get $k > 41.3$, so the good values are $k = 42, 43$, and 44. This leads to the three positive solutions $(x, y) = (16, 10), (9, 25)$, and $(2, 40)$.

9. NTG, Exercise 2.11.24.

The base case is given: $\gcd(c, d) = 1$. Suppose we know that $\gcd(c, d^n) = 1$. We want to show that $\gcd(c, d^{n+1}) = 1$ as well.

We know there exist integers r and s such that $cr + ds = 1$. Let g be a common divisor of c and d^{n+1}. Then $g|c$, so $c = gx$ for some integer x. So we have $g(xr) + ds = 1$, which shows $\gcd(g, d) = 1$. Now rewrite $g|d^{n+1}$ as $g|(d^n d)$. Since $\gcd(g, d) = 1$ we can conclude $g|d^n$. So g is a common divisor of c and d^n. By the induction hypothesis, it follows that $g = 1$. So the only common divisor of c and d^{n+1} is 1, which is what we needed to show.

10. Let

$$S = \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n}.$$

Prove that S is not an integer. (Hint: probably the easiest way is to show that the denominator is divisible by 2.)

This was the hardest one! Here are two possible ways to do it:

Slick argument: Let L be the product of all the odd numbers up to n, let k be the largest integer such that 2^k is less than or equal to n, and let $M = 2^{k-1}L$. Consider the product MS, term by term:

- If m is less than or equal to n and is not equal to 2^k, then it is either 2^a for some $a < k$ or it is $2^a x$ with x odd. We need to see that in the latter case we must have $a < k$ also. Indeed, if $a = k$ and $x > 1$ then $2^k x \geqslant 2^k \times 2 = 2^{k+1} > n$. Hence, in all of these cases $M(1/m)$ is an integer.
- The only other m is 2^k itself. But $M2^k =$ (odd)/2, and hence is not an integer.

Since the sum of a bunch of integers and a fraction (odd)/2 can't be an integer, we see that MS is not an integer, and therefore neither is S.

Step-by-step argument: We first need to prove a Lemma, which is easy so I will leave the proof to you. If p is a prime number, we'll say something is exactly divisible by p^a if it is divisible by p^a but not by p^{a+1}.

Lemma. If we add two fractions in lowest terms, one with denominator exactly divisible by 2^a and the other with denominator *not* divisible by 2^a, then the sum, in lowest terms, has denominator exactly divisible by 2^a.

Given the Lemma it's an easy induction argument to show that the denominator can only get more and more divisible by 2 as we add more terms. At each step we are always in the situation of the Lemma. We start with $1/2$ and each step, according to the Lemma, will either make the denominator more divisible by 2 (if the new term is the one divisible by 2^a) or keep it just as divisible as it was before (if not), the sum will never be an integer.

(The crucial bit of the argument is similar to the estimates we did for the slick part: it works because 2^{k+1} sits between 2^k and the next number with the same number of twos in the denominator, namely 3×2^k.)

By the way, one can also make an argument based on showing that if p is a prime between $n/2$ and n, then p divides the denominator but not the numerator of the sum. This is pretty straightforward *provided one knows that such a p exists*. Do you think one always does? Why?

11. Are there any prime numbers p of the form $p = n^3 - 1$? If so, how many of them are there?

Well, yes: $n = 2$ yields $p = 7$ and $n = -1$ yields $p = -2$, which is also a prime. No other values of n work, because of the factorization

$$n^3 - 1 = (n - 1)(n^2 + n + 1).$$

So if $n^3 - 1$ is prime, one of the two factors must be 1, which happens only for $n = 2$, $n = 0$, and $n = -1$. For $n = 0$ we get $n^3 - 1 = -1$, which is a unit, not a prime. So this expression has two prime values, one value that is a unit, one that is zero, and is composite in every other case.

12. Show that the only n such that n, $n + 2$, and $n + 4$ are all primes is $n = 3$.

This is correct only if we assume $n > 0$. As we'll see below, there's one more possibility if we allow n to be negative.

Dividing by 3 we see that $n = 3q + r$, where $r = 0$, 1, or 2. Consider each case separately.

- Suppose $n = 3q$. Then n can only be prime if $q = \pm 1$. If $q = -1$, then $n = -3$ and $n + 2 = -1$ is not prime. If $q = 1$ then $n = 3$ and we get the expected triple $(3, 5, 7)$.

- Suppose $n = 3q + 1$. Then $n + 2 = 3q + 3$ will be divisible by 3, so can only be prime if it is ± 3, which happens for $q = 0$ and $q = -2$. If $q = 0$, $n = 1$ is not prime. If $q = -3$, $n = 3q + 1 = -5$ is prime, but $n + 4 = -1$ is not.

- Suppose $n = 3q + 2$. Then $n + 4 = 3q + 6$ will be divisible by 3, hence can only be prime if $q = -1$ or $q = -3$. If $q = -1$ then $n = 3q + 2 = -1$ is not prime. But if $q = -3$ then $n = 3q + 2 = -7$ is prime, and so are -5 and -3, giving the unexpected solution $(-7, -5, -3)$, which of course is just the mirror image of the expected one.