MA357, Spring 2020 — Problem Set 3 Solutions

1. NTG, Exercise 2.11.36.

Suppose $\gcd(a, b) = 1$ and ab is a square. Write out the factorizations of a and b:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$
$$b = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}$$

Since $\gcd(a, b) = 1$ the lists $\{p_1, p_2, \ldots, p_n\}$ and $\{q_1, q_2 \ldots, q_m\}$ are disjoint, so the factorization of ab is just

$$ab = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}.$$

Since ab is a square, we know that all the exponents in its factorization are even. So all a_i are even and all b_j are even. But then all the exponents in the factorizations of a and b even, so they are both are squares.

Hard question: can it be done *without* using unique factorization?

2. The *least common multiple* of two integers a and b is the smallest positive number divisible by both a and b. The usual notation is $\operatorname{lcm}(a, b)$. Prove that

$$\gcd(a, b)\ \operatorname{lcm}(a, b) = ab.$$

(This is easy using unique factorization, a little bit harder without it.)

Let $d = \gcd(a, b)$, so that $a = a'd$, $b = b'd$ and $\gcd(a', b') = 1$.

Suppose m is a common multiple of a and b. Then in particular it is divisible by a, so that $m = ax = a'dx$. We know that $b|m$, so that $(b'd)|(a'dx)$. Then $b'|a'x$, and since $\gcd(a', b') = 1$ we conclude $x = b'y$. Hence any common multiple looks like $m = a'b'dy$ with $y \in \mathbb{Z}$. The smallest common multiple is the one with $y = 1$, so we get

$$\operatorname{lcm}(a, b) = a'b'd = \frac{ab}{d} = \frac{ab}{\gcd(a, b)},$$

which is what we wanted to prove.

The version with unique factorization goes like this. Suppose we have factorizations of both a and b; allowing 0 as an exponent, we can write them as

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$
$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

Then it's clear that

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$
$$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

So the result we want boils down to

$$\min(a_i, b_i) + \max(a_i, b_i) = a_i + b_i,$$

which is clearly true.

3. Suppose $n, m \in \mathbb{N}$ and write out their prime factorizations:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$
$$m = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

with $a_i \geqslant 0$, $b_i \geqslant 0$ (we allow exponent zero in order to be able to use the same list of primes for both numbers). Find the prime factorizations of $\gcd(n, m)$ and $\operatorname{lcm}(m, n)$.

See the previous solution (up to notation).

4. Show that if $q = 2^n - 1$ is prime, then n must be prime. Find examples to show that when n is prime then $2^n - 1$ may or may not be prime. (Hint: think factorizations.)

The key observation is the identity

$$x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + \cdots + x + 1).$$

If n is not prime, write $n = mk$ with $m > 1$. Then, since $2^{mk} = (2^m)^k$,

$$2^{mk} - 1 = (2^m - 1)(2^{m(k-1)} + \cdots + 2^m + 1).$$

Since $m > 1$, $2^m - 1 \neq 1$, so this gives a nontrivial factorization of $2^{mk} - 1$, which is therefore not prime. So $2^n - 1$ can only be prime if n is prime.

For the examples, $2^2 - 1 = 3$ is prime, but $2^{11} - 1 = 23 \cdot 89$ is not prime. Primes of the form $2^p - 1$ are known as *Mersenne primes*.

5. Suppose a is an integer, $a \geqslant 2$, $n > 0$, and $a^n + 1$ is prime. Show that n is a power of 2. (Same hint!)

First, $n = 1$ is a power of 2 and of course any prime is of the form $a + 1$ for some a. Not much fun here.

If $n > 1$ is odd then we need the identity

$$x^n + 1 = (x + 1)(x^{n-1} - x^{n-2} + x^{n-3} - \cdots + x^2 - x + 1).$$

(One way to see that such an identity must exist is to notice that when n is odd -1 is a root of $x^n + 1$.) Let $x = a \geqslant 2$. Since $2 < a + 1 < a^n + 1$, we get a nontrivial factorization of $a^n + 1$. So when n is odd and $n > 1$ we have shown $a^n + 1$ cannot be prime.

If n is even but not a power of 2, then $n = 2^b k$ with $k > 1$ odd and $b \geqslant 1$. Now the same factorization formula can be used: $a^n + 1 = (a^{2^b})^k + 1$ and making $x = a^{2^b}$ gives you a factorization of $a^n + 1$, which cannot be trivial because $2 < a^{2^b} + 1 < a^n - 1$ (for the last inequality we use $k > 1$). So $a^n + 1$ can't be prime unless n is a power of 2.

6. Let p be a prime number. Suppose $q = 2^p - 1$ is prime, and let $n = 2^{p-1}q$.

a. Find all the positive proper divisors of n. (A divisor d of n is proper if $d \neq n$.)

If q is a prime, then any divisor of $2^n q$ must be either a power of 2 or a power of 2 times q (by unique factorization!). This gives the list

$$1, 2, 2^2, \ldots, 2^{p-2}, 2^{p-1}, q, 2q, 2^2 q, \ldots, 2^{p-2}q,$$

where the last one, $2^{p-1}q$, is not there because it's not a proper divisor.

b. Show that the sum of the proper divisors of n is equal to n.

The formula for the sum of a gemetric progression shows at once that

$$1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$$

(or just write the first number in binary and see what happens when you add 1). So the sum of all the proper divisors of $2^{p-1}q$ is

$$1 + 2 + 2^2 + \cdots + 2^{p-1} + q + 2q + 2^2 q + \cdots + 2^{p-2}q.$$

Factoring out q from the second half, using the summation formula, and remembering that $q = 2^p - 1$ gives

$$2^p - 1 + (2^{p-1} - 1)q = q + 2^{p-1}q - q = 2^{p-1}q,$$

as claimed.

c. Find the first three n of this form.

The first three primes work:

- $2^2 - 1 = 3$ gives $n = 6$
- $2^3 - 1 = 7$ gives $n = 28$
- $2^5 - 1 = 31$ gives $n = 496$

Numbers n such that the sum of the proper divisors of n is equal to n are known as *perfect numbers*. The numbers you will find are the three smallest perfect numbers.

Euler proved that all even perfect numbers are obtained this way. What about *odd* perfect numbers?

7. For any positive integers n, let $\sigma_0(n)$ be equal to the number of positive divisors of n. Show that if $\gcd(n, m) = 1$ then $\sigma_0(mn) = \sigma_0(m)\sigma_0(n)$. (Functions with this property are called *multiplicative*.)

In class we found a formula for $\sigma_0(n)$ in terms of the prime factorization of n. Since the prime factorizations of n and m have no factors in common, it's easy to see from that formula that $\sigma_0(mn) = \sigma_0(m)\sigma_0(n)$.

An alternative approach would be to show that any divisor of mn must be equal to de where $d|m$ and $e|n$, and this decomposition is unique. That isn't hard to prove.

It's worth noticing that $\sigma_0(2) = 2$ but $\sigma_0(4) = 3 \neq \sigma_0(2)\sigma_0(2)$, so the assumption that $\gcd(m, n) = 1$ is essential.

8. NTG, Exercise 3.5.3. (This is a good example of "it worked once, maybe the same idea will work again.")

Notice first that if we multiply two numbers of the form $4k + 1$ we get a number of the same form. (In congruence language, if $a \equiv 1 \pmod 4$ and $b \equiv 1 \pmod 4$, then $ab \equiv 1 \pmod 4$.) So a number $N \equiv -1 \pmod 4$ must have at least one prime divisor that is $\equiv -1 \pmod 4$.

Now just follow the earlier proof: give a list $p_1, p_2, \ldots, p_k$ of primes that are congruent to -1 mod 4, let $N = 4p_1p_2 \cdots p_k - 1$. Then $N \equiv -1 \pmod 4$, so it must be divisible by a prime $q \equiv -1 \pmod 4$, and q cannot be equal to any of the p_i.

9. NTG, Exercises 3.5.10 and 3.5.11.

These are both dartardly tricks.

If $17p + 1 = n^2$, then $17p = n^2 - 1 = (n + 1)(n - 1)$ so either $n + 1 = 17$ or $n - 1 = 17$. If $n - 1 = 17$, we get $p = n + 1 = 19$. If $n + 1 = 17$, we get $p = n - 1 = 15$, which is not prime. So the only such prime is 19 And indeed $17 \cdot 19 + 1 = 324 = 18^2$.

If $p + 1 = n^3$ then $p = n^3 - 1$, which reduces us to the previous problem set.

10. Show that no square has last digit 2, 3, 7, or 8.

If the last digit of n is a, then $n = 10x + a$, so $n \equiv a \pmod{10}$, so what the question is asking us to do is show that $n^2 \pmod{10}$ must be one of the values listed. But that's easy: list all 10 possible "residues" $\pmod{10}$ and square each. You can save some work by noticing that $a^2 = (-a)^2$, so that you actually only need to square $0, 1, 2, 3, 4, 5$. The answers are $0, 1, 4, 9, 6, 5 \pmod{10}$, so any square must end in one of those digits.

11. Suppose m and n are relatively prime, i.e., $\gcd(m, n) = 1$. Show that to say $a \equiv b \pmod{mn}$ is equivalent to the pair of congruences $a \equiv b \pmod m$, $a \equiv b \pmod n$.

Translating back from congruences into divisibility, what we need to prove is that mn

divides $b - a$ if and only if both m and n do. So in fact we'll prove that in general:

Lemma: Let K be an integer and suppose $\gcd(m, n) = 1$. Then $mn|K$ if and only if both $m|K$ and $n|K$.

Proof: One direction is easy. If $mn|K$, then $K = mnx = m(nx) = n(mx)$, so $m|K$ and $n|K$. The important part is to show the converse.

Converse 1 (Fancy): So suppose $m|K$ and $n|K$. Then $K = my = nz$ for some integers y and z. But n is clearly a divisor of $nz = my$, so we see that $n|my$. Since $\gcd(m, n) = 1$, we get that $n|y$. Hence $y = nx$ and $K = my = mnx$. So $mn|K$.

Converse 2 (Brute Force): Consider the prime factorization of K. It must contain the prime factorization of m and also the prime factorization of n. But $\gcd(m, n) = 1$ means that these two are disjoint, and together they make up the factorization of mn. So inside the factorization of K we can find the factorization of mn, showing that $mn|K$.

12. NTG, Exercise 4.7.10.

Notice first that if n is even we have $n^2 \equiv 0 \pmod 4$, while if n is odd we have $n^2 \equiv 1 \pmod 4$. Since a, b, c are not all even, the only possibility for $a^2 + b^2 = c^2 \pmod 4$ is $0 + 1 = 1$. Hence one of a and b is even and the other is odd. And c is also odd.

13. Suppose we have $a^2 + b^2 = c^2$ with $\gcd(a, b, c) = 1$. In the previous problem you showed that one of a and b must be even (and the other odd). Suppose b is even.

a. Show that $\gcd(a, b) = 1$ and likewise for the other pairs. In particular, a and c are odd.

   Let p be a prime. If $p|a$ and $p|b$, then also $p|(a^2+b^2)$, so $p|c^2$, so $p|c$, contradicting the assumption that $\gcd(a, b, c) = 1$. So $\gcd(a, b) = 1$. Similarly for the other pairs.

b. Rewrite the equation as $b^2 = c^2 - a^3 = (c+a)(c-a)$. What is $\gcd(c+a, c-a)$?

   We solved this in Problem Set 2: since a and c are odd, $\gcd(c + a, c - a) = 2$.

c. Use Problem 1 to conclude that there exist u, v such that $c + a = 2u^2$ and $c - a = 2v^2$.

   Write $b = 2k$, $c + a = 2n$, $c - a = 2m$, and we know $\gcd(m, n) = 1$. Then our equation

$$b^2 = c^2 - a^3 = (c + a)(c - a)$$

becomes

$$4k^2 = 4mn,$$

so $mn = k^2$. By problem 1, it follows that both m and n are squares, so $m = u^2$, $n = v^2$.

d. Solve for b in terms of u and v.

We have $b^2 = 4k^2 = 4u^2v^2$, so $b = 2uv$.

e. Find all integer solutions $a^2 + b^2 = c^2$ such that $\gcd(a, b, c) = 1$.

We showed that if $a^2 + b^2 = c^2$ then there exist u, v such that $c + a = 2u^2$, $c - a = 2v^2$, so $c = u^2 + v^2$ and $a = u^2 - v^2$. Since a and c are odd and relatively prime, we also see that u and v are relatively prime and cannot both be odd. So

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2).$$

Conversely, if a, b, c are of that form it's easy to check that they satisfy the equation. So as u and v run through all pairs of relatively prime integers that are not both odd, this formula gives all solutions.