1 List of problems to consider

1. We say that two primes p, q are *twin primes* if $|p-q| = 2$. For example, $11, 13$ are twin primes, as are $29, 31$. How many primes less than 100 are twins? Less than 200? Are there infinitely many?

   Solution: The twin primes less than 100 are $(3,5), (5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$, $(71,73)$. The ones less than 200, in addition to those less than 100, are $(101,103)$, $(107,109)$, $(137,139)$, $(149,151)$, $(179,181)$, $(191,193)$, $(197,199)$.

   Whether or not there are infinitely many is an open problem, called the *Twin Prime conjecture*. It is suspected to be true, but not known.

2. Prove or disprove: There do not exist three integers n, $n+2$, $n+4$, all of which are prime.

   Solution: This is false. 3, 5, 7 (i.e. $n = 3$) are all prime.

3. Prove or disprove: For every integer n, the integers $2n$ and $4n+3$ are relatively prime. [Hint: Remember that if $d \mid a$ and $d \mid b$, then $d \mid (sa + tb)$ for any integers s, t.]

   Solution: This is false. If $3 \mid n$, then $3 \mid 2n$ and $3 \mid (4n + 3)$. For example, if $n = 3$ then $2n = 6$ and $4n + 3 = 15$, and $\gcd(6, 15) = 3$.

4. Prove or disprove: For every integer n, the integers $2n + 1$ and $3n + 2$ are relatively prime. [Hint: Same as above.]

   Solution: This is true. Suppose that $d \mid (2n + 1)$ and that $d \mid (3n + 2)$. Then we have that

   $$\begin{aligned} d &\mid \big((3n+2) - (2n+1)\big) = n + 1 \\ d &\mid \big(2(2n+1) - (3n+2)\big) = n \end{aligned}$$

   and so $d \mid n$ and $d \mid (n + 1)$. From class we know that this implies that $d = 1$.

5. Prove or disprove: If p, q are primes with $p, q \geq 5$, then $p^2 - q^2$ is divisible by 24.

   Solution: We first consider what possible remainders primes may have upon division by 24. The only possiblities are, for $p \geq 5$, (easy to check): 5,7,11,13,17,19,23. If we square each of these and look at the remainder of those upon division by 24 are all 1! Thus $p^2 = 24a + 1$ and $q^2 = 24b + 1$, and so $p^2 - q^2 = 24(a - b)$ as claimed.

6. The greatest common divisor of a, b was defined previously as the... greatest divisor that a and b have in common. Similarly, the least common multiple is defined to be the smallest multiple of both a and b; for example, if $a = 4$ and $b = 6$, then $gcd(a, b) = 2$ and $lcm(a, b) = 12$.

   Prove or disprove: For every integers a, b, we have that

   $$lcm(a, b)gcd(a, b) = ab$$

   [Hint: Look at the fundamental theorem of arithmetic. Can you use that to figure out what $gcd(a, b)$ and $lcm(a, b)$ are?]

Solution: Write $a = p_1^{a_1} \cdots p_k^{a_k}$ and $b = p_1^{b_1} \cdots p_k^{b_k}$ (with $a_i, b_i \geq 0$—this allows us to use the same list of primes for both a and b). Then it is easy to see that

$$gcd(a,b) = p_1^{\min(a_1,b_1)} \cdots p_k^{\min(a_k,b_k)}$$
$$lcm(a,b) = p_1^{\max(a_1,b_1)} \cdots p_k^{\max(a_k,b_k)}$$

Since $a_i + b_i = \min(a_i, b_i) + \max(a_i, b_i)$, the conclusion follows.

7. Show that there are no strictly positive integer solutions to the equation

$$x^2 - y^2 = 1$$

(Hint: Factor the left-hand side). Are there any solutions if we allow x, y to be negative or zero?

Solution: We are trying to solve $(x-y)(x+y) = 1$. The only possible solution is $x+y = 1 = x-y$, or $x+y = -1 = x-y$, which has as integer solutions $x = \pm 1, y = 0$ or $y = \pm 1, x = 0$. But these do not satisfy the given constraint.

8. Find *all* integer solutions to the equation $x^2 - y^2 = 10$.

Solution: Similar to before, we factor this as $(x-y)(x+y) = 10$. Since 10 has as factorization $1 \cdot 10$ and $2 \cdot 5$, we have the following possibilities for the pair (x, y).

$$\begin{array}{cccc} (1,10) & (10,1) & (-1,-10) & (-10,-1) \\ (2,5) & (5,2) & (-2,-5) & (-5,-2) \end{array}$$

We will solve $(x, y) = (1, 10)$ and $(x, y) = (2, 5)$, as the rest all arise from swapping x and y or by switching signs. In the first case, we have

$$x + y = 1$$
$$x - y = 10$$

which yields that $2x = 11$, which has no integer solutions. So this cannot happen. In the second we have

$$x + y = 2$$
$$x - y = 5$$

which yields that $2x = 7$ which also has no integer solutions. So there are no integer solutions to the equation $x^2 - y^2 = 10$.

9. Prove or disprove that every even number greater than 2 can be written as a sum of two primes.

Solution: This is called *Goldbach's conjecture*, and it is also a famous open problem.

10. Show that there are no rational roots to the cubic equation $x^3 + x + 1 = 0$. (Hint: What would happen if you assumed there was, and cleared denominators? What can we say about the *parity* [evenness or oddness] of the result?)

Solution: Suppose that there were a rational root $x = \frac{p}{q}$ (with $gcd(p,q) = 1$) to this equation. That is,

$$\frac{p^3}{q^3} + \frac{p}{q} + 1 = 0$$

or

$$p^3 + pq^2 + q^3 = 0$$

for some integers p, q with $q \neq 0$. If p, q are odd, then p^3, pq^2, and q^3 are odd. But then their sum would be odd, which is a contradiction.

If p were even, and q odd, then p^3 and pq^2 are even, but q^3 is odd, which is also a contradiction. A similar result occurs if p is odd and q is even.

11. We say that an integer a has an *inverse* mod b if there is some other integer c such that

$$[a]_b[c]_b = [1]_b$$

What conditions are there on a and b such that we can find such an inverse? [Hint: Look at the Euclidean algorithm]

Solution: The exact conditions are that $gcd(a,b) = 1$. In that case, we can write

$$ac + bd = 1$$

for some integers c, d, and so reduction mod b yields that this is equivalent to

$$[a]_b[c]_b = \underbrace{[b]_b}_{=[0]_b}[d]_b = [1]_b$$

as claimed. Conversely, if we can write $[a]_b[c]_b = [1]_b$ that we can write 1 as a linear combination of a and b, which implies that $gcd(a,b) = 1$.

12. We say that a number is *perfect* if the sum of its proper divisors is itself. For example, 6 and 28 are perfect, since $1 + 2 + 3 = 6$, and $1 + 2 + 4 + 7 + 14 = 28$. Prove the following: If $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is perfect. Is the converse true?