PROBLEM-SOLVING AND PROOFS
ASSIGNMENT 6 SOLUTIONS

(1) Let $a, b \in \mathbb{Z}$.
(a) Prove that $\gcd(a+b,\, a-b) = \gcd(2a,\, a-b) = \gcd(a+b,\, 2b)$.
(b) Suppose that $\gcd(a,\, b) = 1$. What can you say about $\gcd(a^2,\, b^2)$? What about $\gcd(a,\, 2b)$?

Solution.
(a) Recall that $\gcd(x,\, y) = \gcd(x-y,\, y)$.[1]
Setting $x = 2a$, $y = a - b$ gives $\gcd(2a,\, a-b) = \gcd(a+b,\, a-b)$.
Setting $x = 2b$, $y = a + b$ gives $\gcd(2b,\, a+b) = \gcd(b-a,\, a+b)$.
However, the set of divisors of $b - a$ and $a - b$ are the same, so $\gcd(b-a,\, a+b) = \gcd(a-b,\, a+b)$. Hence $\gcd(2b,\, a+b) = \gcd(a-b,\, a+b)$ and the result follows.

(b) Let $a = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ and $b = q_1^{\beta_1} \dots q_n^{\beta_n}$ be the prime factorisations. The statement $\gcd(a,\, b) = 1$ is equivalent to saying that each of the primes p_i and q_j are different.

Squaring a number is the same as doubling the exponents of each prime factor: $a^2 = p_1^{2\alpha_1} \dots p_m^{2\alpha_m}$, $b^2 = q_1^{2\beta_1} \dots q_n^{2\beta_n}$. The prime factors of a^2 will remain different from the prime factors of b^2, so $\gcd(a^2,\, b^2) = 1$.

Multiplying by 2 appends a factor of 2 in the prime factorisation. There are two cases:
- If 2 is a prime factor in the factorisation of a (when a is even), then none of the factors q_i equal 2. Thus $2b = 2^1 q_1^{2\beta_1} \dots q_n^{2\beta_n}$ shares exactly one prime factor with $a = 2^{\alpha_1} \dots p_m^{\alpha_m}$ in 2^1. In this case, $\gcd(a,\, 2b) = 2$.
- The other case is when 2 is not a prime factor of a (when a is odd). All the prime factors of $2b$ are different to prime factors of a, so $\gcd(a,\, 2b) = 1$.

Therefore, $\gcd(a,\, 2b) \in \{1, 2\}$.

(2) The royal treasury has 500 7-ounce weights, 500 11-ounce weights, and a balance scale. An envoy arrives with a bar of gold, claiming it weights 500 ounces. Can the treasury determine whether the envoy is lying? If so, how? What if the weights are 6-ounce and 9-ounce weights?

Solution. The problem can be recast into finding integer solutions of

$$7m + 11n = 500, \tag{1}$$

if we are comparing the bar of gold which allegedly weighs 500 oz, to m 7-oz weights and n 11-oz weights.

Note that $\gcd(7, 11) = 1$ and 500 is divisible by 1.[2] Therefore, this linear Diophantine equation is solvable in integers. We just need to make sure the royal treasury has enough of each weight necessary to measure out 500 oz. After all, if the treasury only has, for example, ten of each weight, then the combined mass of the weights does not reach 500 oz at all. So we should exhibit a way to solve equation (1) when $|m|, |n| \leq 500$ (the number of weights).

The quickest and simplest method is to just guess possible combinations, which is fast for small numbers. For instance, 500 is not divisible by 7, nor $(500 - 11)$, nor $(500 - 2 \cdot 11)$, etc., but $(500 - 6 \cdot 11)$ is divisible by 7. From this, a solution can be obtained: $m = 62$, $n = 6$. Therefore the treasury can check the veracity of the envoy's claim by comparing the gold bar to 62 7-oz weights and 6 11-oz weights.

Here, we will present a more systematic method to solve these types of equations using the (extended) Euclidean algorithm, which is faster (than guessing) for larger numbers. Applying

[1] Can you prove this yourself? If not, ask a friend, a tutor, or see page 126 of the textbook for a proof of this fact.
[2] The proof of this statement is left as an exercise to the reader.

the algorithm to 11 and 7 gives:

$$\begin{aligned} 11 &= 1 \times 7 + 4; \\ 7 &= 1 \times 4 + 3; \\ 4 &= 1 \times 3 + 1; \\ 3 &= 3 \times 1 + 0. \end{aligned}$$

This reaffirms our statement that $\gcd(11, 7) = 1$. Reversing the steps of Euclid's algorithm gives:

$$\begin{aligned} 1 &= 1 \times 4 - 1 \times 3 \\ &= 1 \times 4 - 1 \times (1 \times 7 - 1 \times 4) \\ &= 2 \times 4 - 1 \times 7 \\ &= 2 \times (1 \times 11 - 1 \times 7) - 1 \times 7 \\ &= 2 \times 11 - 3 \times 7. \end{aligned} \tag{2}$$

If we want to solve equation (1), multiply (2) by 500 to obtain a solution $m = -1500$, $n = 1000$. These number of weights are too large for our treasury, but from this solution, more solutions can be formed: $m = -1500 + 11k$, $n = 1000 - 7k$, for $k \in \mathbb{Z}$. From inspection, $k = 100$ works: $m = -400$, $n = 300$. This amounts to balancing the bar of gold and 400 7-oz weights on one side, against 300 11-oz weights.

Suppose instead the treasury only had 6 oz and 9 oz weights. The equation we want to solve in integers is

$$6m + 9n = 500. \tag{3}$$

In contrast to the previous problem, $\gcd(6, 9) = 3$ and 500 is *not divisible* by 3, so (3) cannot be solved in integers. The treasury should just go out and buy a set of weighing scales instead.

(3) Show that the gaps between primes can be arbitrarily large. Do this by constructing, for any positive integer n, a set of n consecutive integers that are not prime. (Hint: Determine a positive integer x such that x is divisible by 2, $x+1$ is divisible by 3, $x+2$ is divisible by 4, etc.)

Solution. Our aim is to construct n consecutive composite numbers for any given n. Using the hint, let's try to find a number x such that $(x+k-1)$ is divisible by $(k+1)$ for $k = 1, 2, \ldots, n$.

If $(x+k-1)$ is divisible by $(k+1)$, then $(x+k-1)-(k+1) = x-2$ must also be divisible by $(k+1)$. So can we find an x such that $(x-2)$ is divisible by all of $2, 3, \ldots, n+1$? Yes, by using $x = (n+1)! + 2$. The integers $(n+1)! + 2$, $(n+1)! + 3$, $\ldots$, $(n+1)! + (n+1)$ give the desired sequence of n consecutive composite numbers.

(4) Let p be a prime number.
(a) Prove that p divides $\binom{p}{k}$ for any $1 \leq k \leq p-1$.
(b) Prove that $n^p - n$ is divisible by p for every $n \in \mathbb{N}$. (Hint: Use the binomial theorem and part (a) in a proof by induction.)

Solution.
(a) The value of the binomial coefficient $\binom{p}{k}$ is

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

If we write out the prime factorisation of the numerator, we can find a single factor of p, coming from the multiplicand p in the product $p!$. However, the denominator does not have any factor of p. This is because both k and $p-k$ are strictly less than p (remember $1 \leq k \leq p-1$), so $k!$ and $(p-k)!$ do not have p as a multiplicand. Therefore, after dividing the numerator by the denominator, the single factor of p remains.

(b) Fix a prime p, and induct on n. When $n = 1$, $n^p - n = 1^p - 1 = 0$, which is evidently divisible by p.

Assume that $n^p - n$ is divisible by p. From the binomial formula,

$$(n+1)^p - (n+1) = \left(\sum_{k=0}^{p} \binom{p}{k} n^k\right) - (n+1) = \left(\sum_{k=1}^{p-1} \binom{p}{k} n^k\right) + (n^p - n).$$

On the right side, each term in the series is divisible by p from part (a), and $n^p - n$ is also divisible by p by the inductive hypothesis. So the left side must also be divisible by p. Therefore, by induction, we have proved $n^p - n$ is divisible by p for all $n \in \mathbb{N}$.