GCD PROBLEMS AND SOLUTIONS

(1) Suppose that \( \gcd(a, b) = 1 \). Prove that \( \gcd(na, nb) = n \).

**Answer:** In fact, we can just as easily prove that if \( \gcd(a, b) = d \), then \( \gcd(na, nb) = nd \). Suppose that \( X \subseteq \mathbb{N} \) is any nonempty subset of the natural numbers, and denote by \( nX \) the set \( \{nx \mid x \in X\} \), i.e. just take everything in \( X \) and multiply it by \( n \). Then it is clear that if \( d \) is the least element of \( X \), then \( nd \) is the least element of \( nX \). Indeed, clearly \( nd \in nX \), since \( d \in X \). If there were anything less than \( nd \) in \( nX \), say \( na < nd \), then we would have that \( a \in X \), and \( a < d \), contrary to our assumption that \( d \) is the least element of \( X \).

Now, apply this to the set \( X = \{xa + yb \mid x, y \in \mathbb{Z}\} \cap \mathbb{N} \), the set of positive integers which are \( \mathbb{Z} \)-linear combinations of \( a \) and \( b \). Then \( \gcd(a, b) \) is the least element of this set; call this \( d \). Now, note that the set of positive integers which are \( \mathbb{Z} \)-linear combinations of \( na \) and \( nb \) is simply \( nX \). Indeed, any \( \mathbb{Z} \)-linear combination \( x(na) + y(nb) \) is simply \( n(xa + yb) \), which is clearly in \( nX \). Conversely, any element of \( nX \), of the form \( n(xa + yb) \), is of the form \( x(na) + y(nb) \), and so is a \( \mathbb{Z} \)-linear combination of \( na \) and \( nb \).

Thus by our observation at the start, the least element of \( nX \), which is the \( \gcd \) of \( na \) and \( nb \), is simply \( nd \).

(2) Prove that \( \gcd(a + b, a - b) = \gcd(2a, a - b) = \gcd(a + b, 2b) \).

**Answer:** The point is that these pairs of integers all have the same set of common divisors, and so they must have the same \( \gcd \). Indeed, suppose that \( d \) divides both \( a + b \) and \( a - b \). Then \( d \) also divides \( (a + b) + (a - b) = 2a \), so it is a common divisor of \( 2a \) and \( a - b \). Conversely, if \( d \) divides both \( 2a \) and \( a - b \), then it also divides \( 2a - (a - b) = a + b \), so it is a common divisor of \( a + b \) and \( a - b \). This shows the first equality.

Similarly, if \( d \) divides both \( a + b \) and \( a - b \), then \( d \) also divides \( (a + b) - (a - b) = 2b \), so \( d \) divides both \( a + b \) and \( 2b \). Conversely, if \( d \) divides both \( a + b \) and \( 2b \), then it also divides \( (a + b) - 2b = a - b \), so it is a common divisor of \( a + b \) and \( a - b \). This shows that \( \gcd(a + b, a - b) = \gcd(a + b, 2b) \).

(3) Suppose that \( \gcd(a, b) = 1 \). Does this determine \( \gcd(a^2, b^2) \)? Does it determine \( \gcd(a, 2b) \)?

**Answer:** The answer to the first question is yes, the \( \gcd \) of \( a^2 \) and \( b^2 \) is necessarily 1. Indeed, if \( a \) and \( b \) have no common prime factors (this is equivalent to \( \gcd(a, b) = 1 \)), then \( a^2 \) and \( b^2 \) have no common prime factors, since the prime factors of \( a^2 \) and \( b^2 \) are the same as the prime factors of \( a \) and \( b \), respectively (they just have twice the
However, this particular argument requires uniqueness of prime factorization, which was not covered, so I would not expect this kind of argument on an exam.

But, question for you: If \( \gcd(a, b) = 1 \), then \( xa + yb = 1 \) for some \( x, y \in \mathbb{Z} \). Can you find some \( x', y' \in \mathbb{Z} \), in terms of \( x, y, a, b \), such that \( x' a^2 + y' b^2 = 1 \)? This should be possible, since we have just argued that \( \gcd(a^2, b^2) = 1 \). IF you could do it then this would prove that \( \gcd(a^2, b^2) = 1 \) without appealing to uniqueness of prime factorization. I tried (not hard) and didn’t see how to do it.

The answer to the second question is no. The gcd of \( a \) and \( 2b \) might be 1, or it might not be. For example, take \( a = 2, b = 3 \). Then \( \gcd(a, b) = 1 \), while \( \gcd(a, 2b) = 2 \). On the other hand, if we take \( a = 3, b = 2 \), then \( \gcd(a, b) = \gcd(a, 2b) = 1 \). (THIS one you ought to be able to do.)

(4) Suppose that \( \gcd(a, b) = 1 \) and that \( a \mid n \) and \( b \mid n \). Prove that \( ab \mid n \).

**Answer:** Again, in 2 minutes of thinking I did not see a way to argue this without appealing to uniqueness of prime factorization. Assuming that, the way we would argue this would be: Since \( a \mid n \), every prime factor of \( a \) is a prime factor of \( n \), occurring in \( n \) with at least as high a multiplicity as it occurs with in \( a \). Ditto for \( b \). Now, since \( a \) and \( b \) have no common prime factors (b/c \( \gcd(a, b) = 1 \)), every prime factor of \( ab \) occurs with multiplicity equal to either its multiplicity in \( a \), or its multiplicity in \( b \), and since contains all of those prime factors with at least those multiplicities, we have \( ab \mid n \). (Don’t worry about this one.)

(5) The least common multiple (lcm) of natural numbers \( a \) and \( b \) is the least natural number divisible by both. Prove that \( \text{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b \).

**Answer:** Again, this seems to require uniqueness of prime factorization. Suppose that the primes are \( p_1, p_2, \ldots \), and suppose that \( a = \prod_{i=1}^{\infty} p_i^{a_i} \) (with \( a_i = 0 \) for all but finitely many \( i \)), and suppose that \( b = \prod_{i=1}^{\infty} p_i^{b_i} \) (with \( b_i = 0 \) for all but finitely many \( i \)). Then \( \gcd(a, b) = \prod_{i=1}^{\infty} p_i^{\min(a_i, b_i)} \), and \( \text{lcm}(a, b) = \prod_{i=1}^{\infty} p_i^{\max(a_i, b_i)} \), while \( ab = \prod_{i=1}^{\infty} p_i^{a_i+b_i} \). Then we just need to note that for any integers \( a_i \) and \( b_i \), \( a_i + b_i = \min(a_i, b_i) + \max(a_i, b_i) \). (Don’t worry about this one.)