M3P14 EXAMPLE SHEET 1

1a. Show that for a, b, d integers, we have $(da, db) = d(a, b)$.
1b. Let n, a, b be integers and suppose that $n|ab$. Show that $\frac{n}{(n,a)}$ divides b.

2a. Express 18 as an integer linear combination of 327 and 120.
2b. Find, with proof, all solutions to the linear diophantine equation $110x + 68y = 14$.
2c. Find a multiplicative inverse of 31 modulo 132.
2d. Find an integer congruent to 3 mod 9 and congruent to 1 mod 49.
2e. Find, with proof, the smallest nonnegative integer n such that $n \equiv 1 \pmod 3$, $n \equiv 4 \pmod 5$, and $n \equiv 3 \pmod 7$.

3. Let m and n be integers. Show that the greatest common divisor of m and n is the unique positive integer d such that:

- d divides both m and n, and
- if x divides both m and n, then x divides d.

(In other rings, we will take these properties to be the *definition* of greatest common divisor.)

4. Least Common Multiples
4a. Let a and b be nonzero integers. Show that there is a unique positive integer m with the following two properties:

- a and b divide m, and
- If n is any number divisible by both a and b, then $m|n$.

The number m is called the *least common multiple* of a and b.
4b. Show that the least common multiple of a and b is given by $\frac{|ab|}{(a,b)}$.

5. Let m and n be positive integers, and let K be the kernel of the map:

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

that takes a class mod mn to the corresponding classes modulo m and n. Show that K has (m, n) elements. What are they?

6. Show that the equation $ax \equiv b \pmod n$ has no solutions if b is not divisible by (a, n), and exactly (a, n) solutions in $\mathbb{Z}/n$ otherwise.

7. For n a positive integer, let $\sigma(n)$ denote the sum $\sum_{d|n, d>0} d$ of the positive divisors of n. Show that the function $n \mapsto \sigma(n)$ is multiplicative.

8. Let p be a prime, and a be any integer. Show that a^{p^2+p+1} is congruent to a^3 modulo p.

9. Let n be a squarefree positive integer, and suppose that for all primes p dividing n, we have $(p-1)|(n-1)$. Show that for all integers a with $(a,n) = 1$, we have $a^n \equiv a \pmod{n}$.

10. Let n be a positive integer. Show that $\sum_{d|n, d>0} \Phi(d) = n$. [Hint: First show that the number of integers a with $0 \leq a < n$ and $(a,n) = \frac{n}{d}$ is equal to $\Phi(d)$.]