PROBLEMS, SHEET 1, MP313, Semester 2, 1999.

1. Use Euclid's division algorithm to calculate $d = \gcd(314, 217)$ and find integers x, y such that $d = 314x + 217y$.

2. Prove that $\gcd(a, b) = 1$ and $a|c$ and $b|c \Rightarrow ab|c$.

3. If $\gcd(a, c) = 1$, prove that $\gcd(a, bc) = \gcd(a, b)$.

4. If $\gcd(b, c) = 1$, prove that
$$\gcd(a, bc) = \gcd(a, b)\gcd(a, c).$$
Show that this also holds under the weaker assumption $\gcd(a, b, c) = 1$.

5. Let $n \geq 1, a \geq 2$. If $a^n + 1$ is prime, deduce that $n = 2^m$.
(Hint:
$$b^{2d+1} + 1 = (b + 1)\sum_{k=0}^{2d}(-1)^k b^k.)$$

6. Let $n > 1, a \geq 2$. If $a^n - 1$ is prime, deduce that $a = 2$ and n is prime.

7. If $a \geq 1, b \geq 1$, prove that $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$. (Hint: Assume $d = \gcd(a, b) = ax - by$, where x and y are positive integers.)

8. (a) If a, $b_1, \ldots, b_n \in \mathbb{Z}$ and $\gcd(a, b_i) = 1$, for $i = 1, \ldots, n$, prove that $\gcd(a, b_1 b_2 \cdot \cdots \cdot b_n) = 1$.
   (b) If a, $b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, use (a) to deduce that prove that $\gcd(a^n, b^n) = 1$.
   (c) If a, $b \in \mathbb{Z}, \gcd(a, b) = 1$ and $a|b$, prove that $a = \pm 1$.
   (d) Use part (c) to prove that if a and b are integers such that $a^n|b^n$, then $a|b$. (Hint: Write $a = dA, b = dB$, where $d = \gcd(a, b)$.)

9. Prove that if $m > n$, then $a^{2^n} + 1$ divides $a^{2^m} - 1$. Also show that if a, m, n are positive integers with $m > n$, then
$$\gcd(a^{2^m} + 1,\ a^{2^n} + 1) = \begin{cases} 1 & \text{if } a \text{ is even,} \\ 2 & \text{if } a \text{ is odd.} \end{cases}$$

10. If $\gcd(a,\ b) = 1$ and p is an odd prime, show that
$$\gcd\left(a + b,\ \frac{a^p + b^p}{a + b}\right) = 1 \text{ or } p.$$
(Hint: Let $t = a + b$ and substitute $a = t - b$ in $a^p + b^p$).

11. If n is composite, prove that $\phi(n) \le n - \sqrt{n}$.

    (Method (a). Let $n = uv$, $1 < u$, $1 < v$, $v \le u$. Then $u \ge \sqrt{n}$. Also the integers v, $2v$ $\ldots, uv$ are each not relatively prime to n .

    Method (b). Let $p \mid n$, p a prime, $p \le \sqrt{n}$. Then $n = p^a v$, $p \not| v$, $a \ge 1$. Also $\phi(v) \le v$.)

12. Let $m > 1, n > 1$. Prove that

$$\phi(mn) = \frac{\phi(m)\phi(n)\gcd(m,n)}{\phi(\gcd(m,n))}.$$

    (Hint: Let $\gcd(m,n) = p_1^{a_1} \cdots p_t^{a_t}$, $a_1 > 0, \ldots, a_t > 0$. Then

$$m = p_1^{b_1} \cdots p_t^{b_t} M \text{ and } n = p_1^{c_1} \cdots p_t^{c_t} N,$$

    where $(M, N) = 1$ and $p_1, \ldots, p_t$ do not divide MN.

13. If $m|n$, show that $\phi(m)|\phi(n)$.

    (Hint: Write $m = p_1^{b_1} \cdots p_t^{b_t}$ and $n = p_1^{c_1} \cdots p_t^{c_t} M$, where M is not divisible by any of $p_1, \ldots, p_t$ and $b_1 \le c_1, \ldots, b_t \le c_t$.)

14. Prove that $\phi(n)$ has the form $4k+2$ if and only if $n = p^a$ or $2p^a$, where p is a prime of the from $4m + 3$.

15. If $n > 1$, prove that sum of the integers x satisfying $1 \le x \le n$ and $\gcd(x, n) = 1$ is $n\phi(n)/2$. (Hint: If x satisfies the conditions, so does $n - x$.)