Number Theory

Sheet 2 — MTH3251

1. Proof that if $\gcd(a, m) = 1 \wedge \gcd(b, m) = 1$ then $\gcd(ab, m) = 1$
2. Proof that if $c|ab \wedge \gcd(a, c) = 1$ then $c|b$
3. Proof that if $\gcd(ak, bk) = k \gcd(a, b)$
4. Proof that $a^m - 1|a^n - 1$ iff $m|n$
5. Proof that $\gcd\left(a^m - 1, a^n - 1\right) = a^{\gcd(m,n)} - 1$
6. Use the extended Euclidean algorithm to find the following
   i. $\gcd(119, 272)$
   ii. $\gcd(12378, 3054)$
   iii. $\gcd(1769, 2378)$
7. Proof that if $\gcd(a, b) = 1$
   i. $\gcd(a + b, a - b) = 1$ *or* 2
   ii. $\gcd(a + b, a^2 + b^2) = 1$ *or* 2
8. Determine if a solution exists for
   i. $6x + 51y = 22$
   ii. $33x + 14y = 115$
   iii. $14x + 35y = 93$
9. Determine all integer solutions of $56x + 72y = 40$
10. If $m|a, b, n$ proof that $ax \equiv b \pmod n$ has solution iff $\bar{a}x \equiv \bar{b} \pmod n$ has solution, were $\bar{a} = \frac{a}{m}, \bar{b} = \frac{b}{m}$.
11. If $m|a, b$ and $\gcd(a, n) = 1$ proof that $ax \equiv b \pmod n$ has solution iff $\bar{a}x \equiv \bar{b} \pmod{\bar{n}}$ has solution, were $\bar{a} = \frac{a}{m}, \bar{b} = \frac{b}{m}, \bar{n} = \frac{n}{m}$.
12. Proof that $ax \equiv b \pmod n$ has solution iff $\gcd(a, n)|b$ and the number of solutions in modulo n is $\gcd(a, n)$.
13. Find all possible solutions for
    i. $10x \equiv 6 \pmod{14}$
    ii. $12x \equiv 18 \pmod{22}$
    iii. $18x \equiv 42 \pmod{50}$