Number Theory Homework #1

1. (a) Show that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

(b) Show that an integer is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. (If $A = a_0 + a_1 10^1 + a_2 10^2 + \ldots$, with $0 \leq a_i \leq 9$, then the alternating sum of digits is $a_0 - a_1 + a_2 - \ldots$.)

2. Compute $\gcd(1369, 2597)$ and write this number as a linear combination of 1369 and 2597.

3. (a) Define $\gcd(a, b, c)$, $a, b, c \in \mathbf{Z}$.

(b) Prove that $\gcd(a, b, c) = \gcd(a, \gcd(b, c))$.

(c) Compute $\gcd(499, 731, 1751)$.

4. (a) Define a least common multiple of $a, b \in \mathbf{Z}$ similar to the definition of a greatest common divisor. (We write $\mathrm{lcm}(a, b)$ for the non-negative least common multiple of a, b.)

(b) Prove that if

$$a = (-1)^{\varepsilon} \prod_p p^{\alpha_p}, \quad b = (-1)^{\delta} \prod_p p^{\beta_p},$$

then

$$\mathrm{lcm}(a, b) = \prod_p p^{\gamma_p}, \text{ where } \gamma_p = \max(\alpha_p, \beta_p).$$

5. (a) Prove that the remainders $r_1, r_2, \ldots$ in the Euclidean algorithm satisfy $r_{i+2} < r_i/2$. (Hint: consider separately the cases $r_{m+1} < r_m/2$, $r_{m+1} = r_m/2$, $r_{m+1} > r_m/2$.)

(b) Prove that if $a, b \in \mathbf{Z}$, $a > b > 0$, $b < 2^n$, then in the Euclidean algorithm for $\gcd(a, b)$ the number of steps (divisions) is not more than $2n$.