Math 104a: Number theory – Problem set 1

François Thilmany

Due Friday 6 July 2018

Problem 1. Prove the following properties of division. Here, a, b, c, d are arbitrary elements of $\mathbb{Z}$.

(a) $a \mid 0$, $a \mid a$ and $\pm 1 \mid a$;
(b) if $a \mid b$ and $b \mid c$, then $a \mid c$;
(c) if $a \mid b$ and $b \mid a$, then $a = \pm b$;
(d) $a \mid b$ and $a \mid c$ if and only if $a \mid (xb + yc)$ for all $x, y \in \mathbb{Z}$;
(e) if $a \mid b$ and $c \mid d$, then $ac \mid bd$;
(f) if $ac \mid bc$ and $c \neq 0$, then $a \mid b$.

Problem 2. Prove that for any $n \in \mathbb{N}$, $5^{2n+1} + 2^{2n+1}$ is divisible by 7.

Problem 3. Prove the following properties of the greatest common divisor, denoted 'gcd'. Here, a and b are arbitrary elements of $\mathbb{Z}$ and $d \in \mathbb{N} - \{0\}$.

(a) $\gcd(a, 0) = |a|$, $\gcd(a, a) = |a|$, and $\gcd(a, \pm 1) = 1$;
(b) $\gcd(a, xa \pm b) = \gcd(a, b)$, for any $x \in \mathbb{Z}$;
(c) if d divides a and b, then $\gcd(\frac{a}{d}, \frac{b}{d}) = \frac{\gcd(a,b)}{d}$.

Use parts (b) and (c) to quickly compute $\gcd(23000, 2310)$.

Problem 4. Let $a, b \in \mathbb{Z}$ be such that $\gcd(a, b) = 1$. Determine the value of $\gcd(a + b, a - b)$ as a function of a and b.

The Fibonacci sequence is the sequence $(F_n \mid n \in \mathbb{N})$ given inductively by

$$F_0 = 0, \quad F_1 = 1 \quad \text{and} \quad F_{n+1} = F_n + F_{n-1} \quad \text{for } n \geq 1.$$

Problem 5. Prove that for any $n \in \mathbb{N}$, $\gcd(F_n, F_{n+1}) = 1$.

Problem 6. Prove that for any $k, n \in \mathbb{N}$ with $k < n$, one has

$$F_n = F_{k+1}F_{n-k} + F_kF_{n-(k+1)}.$$

Deduce that if $m \mid n$, then $F_m \mid F_n$.

Problem 7. Let $a \in \mathbb{Z}$. What are all the possible remainders of the (Euclidean) division of
(i) a^2 by 2;
(ii) a^2 by 3;
(iii) a^2 by 5;
(iv) a^2 by 8;
(v) $a^3 - a$ by 3;
(vi) a^3 by 3;
(vii) a^3 by 5;
(viii) a^3 by 7.

Problem 8. Let a be an odd integer, and assume $a > 1$. Prove that a has a unique representation $a = x^2 - y^2$ as a difference of two squares if and only if a is a prime number.

Problem 9. Let $a, b, c \in \mathbb{Z}$. Prove that
(a) if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$;
(b) if $a \mid c$, $b \mid c$ and $\gcd(a, b) = 1$, then $ab \mid c$.

Problem 10. Let $\frac{a}{b}, \frac{c}{d}$ be two rational numbers in reduced form (i.e. $a, c \in \mathbb{Z}$, $b, d \in \mathbb{N} - \{0\}$ and $\gcd(a, b) = \gcd(c, d) = 1$). Show that if $\frac{a}{b} + \frac{c}{d}$ is an integer, then $b = d$.

Problem 11. Let $a \in \mathbb{Z}$ be both a square and a cube, i.e. there are $b, c \in \mathbb{Z}$ such that $a = b^2$ and $a = c^3$. Prove that a is a sixth power, i.e. there exists $d \in \mathbb{Z}$ such that $a = d^6$.

Let $\mathrm{lcm}(a, b)$ denote the least common multiple of two integers a and b, that is, l is a positive multiple of both a and b, and l divides any other common multiple of a and b.

Problem 12. Let $a, b \in \mathbb{Z}$ and write $a = \pm p_1^{e_1} \dots p_r^{e_r}$, $b = \pm p_1^{f_1} \dots p_r^{f_r}$ their unique factorization as a product of the distinct positive primes $p_1, \dots, p_r$ dividing either a or b. Prove that $\gcd(a, b) = p_1^{\min(e_1, f_1)} \dots p_r^{\min(e_r, f_r)}$ and that $\mathrm{lcm}(a, b) = p_1^{\max(e_1, f_1)} \dots p_r^{\max(e_r, f_r)}$. Deduce that $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = a \cdot b$ for any $a, b \in \mathbb{N}$.

Problem 13. Let $a \in \mathbb{N} - \{0\}$ and write $a = p_1^{e_1} \dots p_r^{e_r}$ its unique factorization as a product of the distinct positive primes $p_1, \dots, p_r$. Determine the number of (positive) divisors of a, in term of the p_i's and the e_i's. Deduce that a is a square if and only if it has an odd number of positive divisors.

Problem 14. Show that there are infinitely many prime numbers whose residues are 3 modulo 4. (Hint: adapt Euclid's proof of the infinitude of prime numbers.)