Problem 1. For positive integers a, b define $[a, b] = ab/\gcd(a, b)$.

a) Prove that $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are relatively prime.

b) Prove that if $a|c$ and $b|c$ then $[a, b]|c$.

c) Conlcude that $[a, b]$ is the smallest positive integer divisible by both a and b (we call it the **least common multiple of** a **and** b).

Solution: a) If $d > 0$ is a common divisor of $a/\gcd(a, b)$ and $b/\gcd(a, b)$ then $d\gcd(a, b)$ divides both a and b and hence $d\gcd(a, b) \leq \gcd(a, b)$. It follows that $d \leq 1$, i.e. $d = 1$. In other words, $a/\gcd(a, b)$ and $b/\gcd(a, b)$ do not have any positive common divisors different from 1, i.e. they are relatively prime.

b) Note that $a|c$ implies that $\frac{a}{\gcd(a,b)}|\frac{c}{\gcd(a,b)}$. Similarly, $\frac{b}{\gcd(a,b)}|\frac{c}{\gcd(a,b)}$. Since by a) the numbers $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are relatively prime, we conclude that their product also divides $c/\gcd(a, b)$. In other words $\frac{ab}{\gcd(a,b)^2}|\frac{c}{\gcd(a,b)}$. It follows that $[a, b] = \frac{ab}{\gcd(a,b)}|c$.

c) Clearly $[a, b]$ is divisible by both a and b. On the other hand, any positive integer divisible by both a and b is according to b) also divisible by $[a, b]$, hence it can not be smaller than $[a, b]$. It means that $[a, b]$ is the lest common multiple of a and b.

Problem 2. Let $F_n = 2^{2^n} + 1$, for $n = 0, 1, 2, ...$

a) Prove that $F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_n = F_{n+1} - 2$ for every n.

b) Prove that $\gcd(F_n, F_m) = 1$ for $n \neq m$.

Solution: a) The easiest proof seems to be by induction on n. Since $F_0 = 3 = 5 - 2 = F_1 - 2$, the result holds for $n = 0$. Suppose that it holds for some $n \geq 0$, i.e.

$$F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_n = F_{n+1} - 2 = 2^{2^{n+1}} - 1.$$

Multiplying both sides by $F_{n+1} = 2^{2^{n+1}} + 1$ we get

$$F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_n \cdot F_{n+1} = (2^{2^{n+1}} - 1)(2^{2^{n+1}} + 1) = 2^{2^{n+2}} - 1 = F_{n+2} - 2.$$

so the result holds for $n + 1$. By induction, it holds for every $n \geq 0$.

b) Suppose that $m < n$ and d is the greatest common divisor of F_m and F_n. Clearly d divides $F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_{n-1}$ (since F_m is one of the factors) and therefore it divides

the difference $F_n - F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_{n-1}$, which is 2 by a). Thus $d|2$, i.e. $d = 1$ or $d = 2$. Hovewer $d = 2$ is not possible, since the numbers F_k are all odd. Hence $d = 1$, i.e. $\gcd(F_n, F_m) = 1$.

Solution to Problem 16 from the textbook: Given integrs m, n let $S = \{xm + yn : x, y \in \mathbb{Z}\}$ be the set of all integers which can be expressed as $xm + yn$ for some integrs x, y.

i) Suppose that $s, t \in S$ and q is any integer. Thus there are intgers x_1, y_1, x_2, y_2 such that $s = x_1m + y_1n$ and $t = x_2m + y_2n$. It follows that $qs = (qx_1)m + (qy_1)n \in S$ and $s + t = (x_1 + x_2)m + (y_1 + y_2)n \in S$. In other words, S is closed under addition and multiplication by any integer.

ii) Suppose that S contains elements different from 0 (note that $S = \{0\}$ iff $m = 0 = n$; why?). Then S contains positive integers (why?). Let d be the smallest positive element of S. We want to prove that S consists exactly of all multiples of d. Clearly any multiple of d is in S, since by i) the set S is closed under multiplicatuion by any integer. Conversly, let $s \in S$. By the divison algorithm, we may write $s = kd + r$ for some integers k, r with $0 \leq r < d$. Thus $r = s + (-k)d$. Since $s, d \in S$, we conclude from i) that $(-k)d \in S$ and $s + (-k)d \in S$. In other words, $r \in S$. Recall that d is the smallest positive element of S and $0 \leq r < d$ is an element of S. Clearly this can be true only if $r = 0$. Thus $d|s$. We proved then that any memember of S is divisible by d, so indeed S consists exactly of multiples of d.

iii) Note that $m = 1 \cdot m + 0 \cdot n$ and $n = 0 \cdot m + 1 \cdot n$ are both in S. By ii), we see then that $d|m$ and $d|n$. Since $d \in S$, we can write $d = xm + yn$ for some integers x, y. If a is any common divisor of m and n then it is also a divisor of $xm + yn = d$. It follows that d is the greatest common divisor of m, n, it is divisible by any other common divisor of m, n and it can be written in the form $xm + yn$. Thuse we have a diiferent proof of the main properties of gcd.

Note: We will get back to this proof later, since almost verbatim it can be used to establish unique factorization in so called principal ideal domains.