Homework 2, solutions

Problem 1. Prove that if a, b are relatively prime integers such that $a|c$ and $b|c$ then $ab|c$. Hint: Write $c = ac_1$, $ua + wb = 1$ for some integers u, w and use this to show that $b|c_1$.

Solution. We folow the hint. Since $a|c$ we have $c = ac_1$ for some integer c_1. Since a, b are relatively prime, there exist integers u, w such that $1 = ua + wb$. Multiplying the last equality by c_1, we arrive at $c_1 = uac_1 + wbc_1 = uc + bwc_1$. Since both uc and bwc_1 are clearly divisible by b, we conclude that $b|c_1$, i.e. $c_1 = bc_2$ for some integer c_2. It follows that $c = ac_1 = abc_2$, so $ab|c_2$.

Problem 2. 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 the numbers $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are relatively prime by part a), we conclude (using Problem 1) 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 3. 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 $n \neq m$.

c) Use b) to give yet another proof that the set of primes is infinite.

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 $n \geq 0$ and the result holds for $0, 1, \ldots, n$. In particular,

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

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. $\gcd(F_n, F_m) = 1$.

c) Each of the numbers F_n has a prime divisor, call it p_n. Since any two among the numbers F_n are relatively prime, no two of the primes p_n can be the same. Thus we have an infinite list of pairwise distinct prime numbers.

Remark. The numbers F_n are called **Fermat numbers**. It is no hard to see that F_0, F_1, F_2, F_3, F_4 are prime numbers. However, Euler proved that F_5 is not a prime. It is still unknown if there exists $n > 4$ such that F_n is a prime number.

Solution to Problem 57 from chapter 1 of the textbook: We only solve part b), part a) follows the same method.

We use the fact that $\gcd(210, 294, 490, 735) = \gcd(210, \gcd(294, \gcd(490, 735)))$. First we compute $\gcd(490, 735)$ using Euclidean algorithm:

$$735 = 1 \cdot 490 + 245; \quad 490 = 2 \cdot 245 + 0.$$

We see that $\gcd(490, 735) = 245$. Working backwards, or using the matrix multiplication method (see the solution to the first quiz), we find that

$$\gcd(490, 735) = 245 = 1 \cdot 735 + (-1) \cdot 490.$$

Now, again using the Euclidean algorithm, we compute $\gcd(294, 245)$:

$$294 = 1 \cdot 245 + 49; \quad 245 = 5 \cdot 49 + 0.$$

We see that

$$\gcd(294, 245) = 49 = 1 \cdot 294 + (-1) \cdot 245.$$

Finaaly, again using the Euclidean algorithm, we compute $\gcd(210, 49)$:

$$210 = 4 \cdot 49 + 14; \quad 49 = 3 \cdot 14 + 7; \quad 14 = 2 \cdot 7 + 0.$$

We see that

$$\gcd(210, 49) = 7 = (-3) \cdot 210 + 13 \cdot 49.$$

We conclude that $\gcd(210, 294, 490, 735) = 7$ and

$$7 = (-3)\cdot 210 + 13\cdot 49 = (-3)\cdot 210 + 13\,(1 \cdot 294 + (-1) \cdot 245) = (-3)\cdot 210 + 13\cdot 294 + (-13)\cdot 245 =$$

$$= (-3)\cdot 210 + 13\cdot 294 + (-13)(1\cdot 735 + (-1)\cdot 490) = (-3)\cdot 210 + 13\cdot 294 + (-13)\cdot 735 + 13\cdot 490.$$