February 28, 2019 Homework 3 due March 7, 2019
Solutions

1. Let $a > b \geq 0$ be integers, and $a = bq + r$, $0 \leq r < b$. Show that $\gcd(a, b) = \gcd(b, r)$.

   Solution. Note that

   a) every divisor d of b and r is also a divisor of a,

   b) every divisor d of a and b is also a divisor of r.

2. Desscribe all positive integers n so that $gcd(n, n + 2) = 2$.

   Solution. Since $2|n$ the number $n = 2m$, and $n + 2 = 2(m + 1)$. If $d|m$ and $d|(m + 1)$, then $d = 1$. Hence for each pair $n, n + 2$ with $n = 2m$ one has $gcd(n, n + 2) = 2$.

3. Let $a, b, c \in \mathbf{N}$, and $d' = \min\{ax + by + cz > 0 \ : \ x, y, z \in \mathbf{Z}\}$. Show that $d|a$, $d|b$, and $d|c$, and for each divisor D of a, b and c one has $D|d$.

   Solution. Let $d' = ax' + by' + cz'$, and $d = ax + by + cz > 0$. Note that $d = d'q + r$ where $0 \leq r < d'$, and $0 \leq r = d - d'q = a(x - qx') + b(y - qy') + c(z - qz') < d'$. Due to minimality of d' one has $d - d'q = 0$, and $d'|d$ for each $D = ax + by + cz > 0$. In particular d' is a divisor of

   $$a = a \cdot 1 + b \cdot 0 + c \cdot 0, \ b = a \cdot 0 + b \cdot 1 + c \cdot 0, \ a = a \cdot 0 + b \cdot 0 + c \cdot 1.$$

   To complete the proof we note that if D is a divisor of a, b and c, then D also is a divisor of $d' = ax' + by' + cz'$.

4. Let p be a prime number. If $\gcd(a, p) = 1$, then $\gcd(a^2, p) = 1$.

   Solution. Assume $\gcd(a^2, p) > 1$. Since p is prime $p = \gcd(a^2, p)$, hence $p|a^2$, and $p|a$.

5. Show that $a^m - 1$ is a composite.

   Solution. $a^m - 1 = (a - 1)(a^{m-1} + a^{m-2} + \cdots + 1)$.

6. Let p be a prime. True or False? $p^m + 1$ is a composite.

   Solution. If $p > 2$, then p is odd, p^m is odd, and $p^m + 1$ is even. If $p = 2$, then $2^1 + 1 = 3$, but $2^3 + 1 = 9$. Let $F_n = 2^{2^n} + 1$. That is $F_0 = 3$, $F_1 = 5$, $F_2 = 17$.

7. Let $F_n = 2^{2^n} + 1$. That is $F_0 = 3$, $F_1 = 5$, $F_2 = 17$.

   a) Show that $\prod\limits_{k=0}^{n-1} F_k = F_n - 2$.

Solution. Use Induction. Note that $F_0F_1 = 15 = 17 - 2 = F_3 - 2$. Assume the statement holds true for $n = k$.

$$\begin{aligned} F_0F_1 \dots F_{k-1}F_k &= (F_k - 2)F_k \\ &= \left(2^{2^k} - 1\right)\left(2^{2^k} + 1\right) \\ &= 2^{2^{k+1}} - 1 = F_{k+1} - 2. \end{aligned}$$

b) Based on the result above can you conclude that F_k and F_n are relatively prime when $k \neq n$?

Solution. If $k \neq n$, and $d = gcd(F_k, F_n)$, then $d|2$, and, since F_k and F_n are odd, d must be 1.