HOMEWORK SET 5. INTRODUCTION TO NUMBER THEORY

1. Let a, b, c, d be integers. Prove the following statements.

a) If $a \mid b$ and $b \mid c$ then $a \mid c$
b) If $a \mid b$ and $b \mid a$ then $a = b$ or $a = -b$.
c) If $a \mid c$ and $b \mid d$ then $ab \mid cd$.
d) If $a \mid b$ and $a \mid c$ then $a \mid xb + yc$ for all $x, y \in \mathbb{Z}$.
e) Suppose that $c \neq 0$. Then $a \mid b$ if and only if $ac \mid bc$.

Solution. **a)** Since $a \mid b$, $b = ka$ for some $k \in \mathbb{Z}$. Since $b \mid c$, $c = mb$ for some $m \in \mathbb{Z}$. Then $c = m(ka) = (mk)a$ and so $a \mid c$.
b) Since $a \mid b$, $b = ka$ for some $k \in \mathbb{Z}$. Since $b \mid a$, $a = mb$ for some $m \in \mathbb{Z}$. In particular, both a, b are non-zero. Then $b = ka = k(mb) = (km)b$ and, since $b \neq 0$, $km = 1$. This implies that $k = m = 1$ or $k = m = -1$.
c) Since $a \mid c$, $c = ka$ for some $k \in \mathbb{Z}$. Since $b \mid d$, $d = mb$ for some $m \in \mathbb{Z}$. Then $cd = (ka)(mb) = (km)ab$ and so $ab \mid cd$.
d) Since $a \mid b$ and $a \mid c$, $b = ma$ and $c = na$ for some $m, n \in \mathbb{Z}$. Then $xb + yc = x(ma) + y(na) = (xm + yn)a$. Thus, $a \mid xb + yc$.
e) Suppose first that $a \mid b$. Then $b = ka$ for some $k \in \mathbb{Z}$ and so $bc = (ka)c = k(ac)$. Thus, $ac \mid bc$.
Conversely, suppose that $ac \mid bc$. Then $bc = kac$ for some $k \in \mathbb{Z}$ and so $c(b - ka) = 0$. Since $c \neq 0$, $b = ka$ and so $a \mid b$.

□

2. Let p be a prime and let $n \in \mathbb{N}$. Find the number of divisors of p^n and their sum.

Solution. By the fundamental theorem of arithmetic, a divisor of p^n is of the form p^a where $0 \leq a \leq n$. Thus, p^n has $n + 1$ divisors, and their sum is $1 + p + p^2 + \cdots + p^n = \frac{p^{n+1}-1}{p-1}$. □

3. Let $p \neq q$ be primes. Find the sum and the number of divisors of pq and their sum.

Solution. By the fundamental theorem of arithmetic, the divisors of pq are 1, p, q and pq. So, pq has 4 divisors, and their sum is $1+p+q+pq = (p+1)(q+1)$. Note that every divisor of pq is a product of a divisor of p and a divisor of q. □

4. (*) Find all integers between 1 and 100 which have exactly 5 different divisors, without finding all divisors of all integers in that range. [*Hint.* Two preceding problems might be helpful.]

5. Find the factorization of $11,227$ [*Hint.* Since $105^2 < 11,227 < 106^2$ and 105 is not a prime, $11,227$ must be divisible by a prime p such that $p < 105$]

Answer. $11,227 = 103 \cdot 109$. □

6. Let n be a positive integer.

a) Show that if n is a perfect square then either $n = 4m$ or $n = 4m + 1$ for some $m \in \mathbb{Z}$.
b) Show that if $n = 4k + 3$ for some $k \in \mathbb{Z}$ then n is not a sum of two perfect squares.
c) Show that no integer in the sequence 11, 111, 1111, 11111, ... is a perfect square or a sum of two perfect squares.

Solution. **a)** Suppose that $n = k^2$ where k is an integer. If k is even then $k = 2l$ for some $l \in \mathbb{Z}$ and so $n = k^2 = 4l^2$. If k is odd then $k = 2l + 1$ for some $l \in \mathbb{Z}$ and so $n = k^2 = (2l + 1)^2 = 4l^2 + 4l + 1 = 4(l^2 + l) + 1$. Since $l^2 + l$ is an integer, it follows that $n = 4m + 1$ for some $m \in \mathbb{Z}$.

(Actually, we can say even more: $l^2 + l = l(l + 1)$ and so is automatically an even number. Thus, $n^2 = 8m' + 1$ for some $m' \in \mathbb{Z}$).

b) We prove the contrapositive. Suppose that $n = a^2 + b^2$ where $a, b \in \mathbb{Z}$. By the previous part, $a^2 = 4m + r$ and $b^2 = 4m' + r'$ with $r, r' \in \{0, 1\}$. Thus, $n = 4q + s$ where $s \in \{0, 1, 2\}$. Therefore, the reminder of n when divided by 4 cannot be 3.

c) We have $11 = 4 \cdot 2 + 3$. All other numbers in this sequence have the form $m \cdot 1000 + 111$, $m \in \mathbb{N}$. Since $4 \mid 1000$ and $111 = 108 + 3 = 4 \cdot 27 + 3$, every number > 11 in our sequence can be written as $4k + 3$ for some k. Thus, all numbers in our sequence are of the form $4n + 3$ and hence are neither perfect squares nor sum of perfect squares by two previous parts.

□

7. Use Euclidean algorithm to find $\gcd(3180, 2148)$ and $\gcd(3123, 2015)$.

Solution. We have

$$\begin{aligned} 3180 &= 2148 + 1032 \\ 2148 &= 2 \cdot 1032 + 84 \\ 1032 &= 12 \cdot 84 + 24 \\ 84 &= 3 \cdot 24 + 12 \\ 24 &= 2 \cdot 12 + 0 \end{aligned} \qquad \begin{aligned} 3123 &= 2015 + 1108 \\ 2015 &= 1108 + 907 \\ 1108 &= 907 + 201 \\ 907 &= 4 \cdot 201 + 103 \\ 201 &= 103 + 98 \\ 103 &= 98 + 5 \\ 98 &= 19 \cdot 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

So, $\gcd(3180, 1032) = 12$ and $\gcd(3123, 2015) = 1$. □

8. Denote by F_n the nth Fibonacci number (so $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$, $n \geq 1$).

a) Use induction to prove that $\gcd(F_n, F_{n+1}) = 1$ and $\gcd(F_n, F_{n+2}) = 1$ for $n > 0$.

Solution. The first claim obviously holds for $n = 1$ and 2. Suppose it is established for all $1 \leq k \leq n$. Suppose that $\gcd(F_{n+1}, F_{n+2}) > 1$. Then there is a prime p such that $p \mid F_{n+1}$ and $p \mid F_{n+2}$. Since $F_{n+2} = F_{n+1} + F_n$ this implies that $p \mid F_n$. But then $\gcd(F_n, F_{n+1}) \geq p$ which is a contradiction.

The second claim obviously holds for $1 \leq n \leq 3$. Suppose it holds for all $1 \leq k \leq n$ and that $\gcd(F_n, F_{n+2}) > 1$. As before, this yields a prime p such that $p \mid F_n$ and $p \mid F_{n+2}$. Then $p \mid F_{n+1}$ for $F_{n+1} = F_{n+2} - F_n$. Then we also have $p \mid F_{n-1}$ since $F_{n-1} = F_{n+1} - F_n$. Then $\gcd(F_{n-1}, F_{n+1}) \geq p$ which is a contradiction. □

b) Use Euclidean algorithm to find $\gcd(F_n, F_{n+1})$ and $\gcd(F_n, F_{n+2})$, $n > 0$.

Solution. Let $n > 2$. We have $F_{n+1} = F_n + F_{n-1}$. Since $0 \leq F_{n-1} < F_n$ (as $F_n = F_{n-1} + F_{n-2}$), we conclude that the remainder of F_{n+1} when divided by F_n is F_{n-1}. Continuing this way we conclude that on each step the remainder is F_k. The algorithm terminates when $k = 0$ since $F_0 = 0$; thus, $\gcd(F_n, F_{n+1}) = F_1 = 1$.

To find $\gcd(F_{n+2}, F_n)$ note that $F_{n+2} = F_{n+1} + F_n = 2F_n + F_{n-1}$. Thus, in Euclidean algorithm we have $r_0 = F_{n+2}$, $r_1 = F_n$, $r_2 = F_{n-1}$. Therefore, $\gcd(F_{n+2}, F_n) = \gcd(F_n, F_{n-1})$. But we already know that $\gcd(F_n, F_{n-1}) = 1$. □

c) Show that, for all $n \geq 0$, F_n is odd if $3 \nmid n$ and F_n is even if $3 \mid n$.

Solution. We use strong induction. The claim is easily verified for $n \leq 3$. Suppose that the claim holds some $n > 3$ and for all for all $0 \leq k < n$. If $3 \mid n$ then $3 \nmid n-1$ and $3 \nmid n-2$ since $n = 3k$ and so $n - 1 = 3(k-1) + 2$ and $n - 2 = 3(k-1) + 1$ and thus have non-zero remainders when divided by 3. Then F_{n-1} and F_{n-2} are both odd by the induction hypothesis and so $F_n = F_{n-1} + F_{n-2}$ is even. If $3 \nmid n$ then either $n = 3k+1$ and then $3 \mid n-1$, $3 \nmid n-2$ or $n = 3k+2$ and then $3 \mid n-2$, $3 \nmid n-1$. In both cases F_{n-1} and F_{n-2} have different parity and so their sum is odd. □

9. Consider the following game. Two players are given several piles of marbles. A move consists in removing three marbles, each one from a *different pile*. The game ends when a move cannot be made (that is, there are less than three piles left). The winner is the person who makes the last move.

Assuming that there were four piles, containing 6, 7, 8 and 11 marbles respectively, can it happen that at the end of the game:

a) only one marble remains?
b) (*) two marbles remain?

Solution. Let N be the total number of marbles at the beginning of the game and write $N = 3q + r$ where $0 \leq r \leq 2$. Since a move consists in removing three marbles, the total number of marbles after k moves is $N - 3k = 3(q-k) + r$ and so *has the same reminder as* N when divided by 3.

If the piles contained 6, 7, 8 and 11 marbles, the total number of marbles at the beginning of the game was $6 + 7 + 8 + 11 = 32 = 3 \cdot 10 + 2$. So, the number of marbles left at the end of the game must have remainder 2 when divided by 3. In particular, the game cannot end with just one marble remaining. □

10. Ten inhabitants of an island populated by knights and knaves were given ten different numbers between 1 and 10.

When asked "Is your number divisible by 2?" three people replied yes.
When asked "Is your number divisible by 4?" six people replied yes.
When asked "Is your number divisible by 5?" two people replied yes.
How many of the ten are knaves and which numbers were given to them?

Solution. People who answer "Yes" to the first question are: knights who were given an even number and knaves who were given an odd number.

People who answer "Yes" to the second question are: knights who were given a number divisible by 4, knaves who were given an odd number and knaves who were given an even number not divisible by 4 (2, 6 or 10).

The difference $(6 - 3 = 3)$ is the number of knaves with even numbers not divisible by 4 minus the number of knights with an even number not divisible by 4. But the sum of these two numbers is also equal to 3; this way we conclude that there are no knights with such numbers and all these numbers (2, 6 and 10) were given to knaves. Two of them (the ones with 2 and 6) answered "Yes" to the last question. This implies that 5 is also given to a knave. This is the only odd number which was given to a knave since a knave with any other odd number would answer "Yes" to the last question, but we already know who answered "Yes" to that question (the knaves with 2 and 6).

We also know that the number of knights who were given a number divisible by 4 plus the number of knaves with odd numbers is 3 (these are the only people who answered "Yes" to the 1st question, since all other even numbers were not given to knights). Thus, there are 2 knights with numbers divisible by 4. We conclude that the numbers are distributed as follows:

1	Knight
2	knave
3	Knight
4	Knight
5	knave
6	knave
7	Knight
8	Knight
9	Knight
10	knave.

$\square$