Mathematics 228(Q1), Assignment 2
Solutions

Exercise 1.(10 marks) A natural number $n > 1$ is said to be square free if $d \in \mathbf{N}$ with $d^2|n$ implies $d = 1$. Show that n is square free if and only if $n = p_1 \cdots p_k$ for distinct primes $p_1, \ldots, p_k$.

Solution. If the prime p occurs more than once in the prime factorization of n then p^2 is a divisor of n with the property $p \neq 1$, hence n is not square-free. We deduce that if n is square-free then the primes occuring in its prime factorization are all distinct.

Conversely, if n is not square-free then it admits a divisor of the form d^2, with $d > 1$. If $n = d^2c$ then, letting

$$d = q_1 \cdots q_i \qquad \text{and} \qquad c = r_1 \cdots r_j$$

be the prime factorizations of d and c, respectively, we deduce

$$n = d^2c = (q_1 \cdots q_i)(q_1 \cdots q_i)(r_1 \cdots r_j)$$

is the prime factorization of n. In particular, the prime q_1 appears twice. We conclude that if the primes occuring in the prime factorization of n are distinct then n is square-free.

Exercise 2.(15 marks) (a) Let $n > 1$ be an integer and suppose

$$a, b \in \mathbf{Z}n + 1 = \{qn + 1 \,:\, q \in \mathbf{Z}\}.$$

Show that the product ab also belongs to $\mathbf{Z}n + 1$.

(b) Let $a \in 4\mathbf{N} + 3 = \{4n + 3 \,:\, n \in \mathbf{N}\}$. Show that a has a positive prime factor in $4\mathbf{N} + 3$. (Hint : If not, what do the positive prime factors of a look like ?)

(c) Show that there are infintely many primes of the form $4n + 3$, $n \in \mathbf{N}$.

Solution.(a) By hypothesis, there exisits integers p and q such that

$$a = pn + 1 \qquad \text{and} \qquad b = qn + 1.$$

We calculate

$$ab = (pn + 1)(qn + 1) = pqn^2 + pn + qn + 1 = (pqn + p + q)n + 1 \in \mathbf{Z}n + 1.$$

(b) Let

$$a = p_1 \cdots p_k$$

the prime factorization of a into a product of positive primes. Since a is odd, being the sum of an even number (in fact, a multiple of 4) and an odd number (namely, 3) all the prime factors p_i are odd. Exercise 3, Assignment 1 allows us to conclude that there is a suitable choice of integer k_i for which p_i has the form $4k_i+1$ or $4k_i + 3$.

If a had no positive prime factor of the form $4k + 3$ then all the factors would be of the form $4k + 1$. Being a product of elements of the form $4k + 1$, part (a) allows us to deduce that a would be of the form

$$a = 4l + 1$$

for some integer l. This contradicts the hypothesis division of a by 4 leaves remainder 3. Therefore, a has a positive prime factor of the form $4k + 1$.

(c) We will prove this statement via an argument similar to that used to prove Theorem 6 in class.Note that 7 is a prime of the desired form. Suppose $p_1, \ldots, p_k$ are distinct positive primes > 3 belonging to $4\mathbf{N}+3$ and consider the integer

$$a = 4p_1 \cdots p_k + 3.$$

By part (b), a admits a positive prime divisor of the form $4k+3$. If p coincided with one of the p_i then

$$p_i|(a-4p_1\cdots p_k)=3,$$

hence $p_i=3$, a contradiction of our assumptions on p_i. Furthermore, if $p=3$ then we would deduce that

$$3|(a-3)=4p_1\cdots p_k$$

which yield the same contradiction. It follows that p is distinct from each p_i and >3.

The preceding procedure allows us to inductively define an infinite sequence of primes >3 of the form $4k+3$, which completes the proof of claim.

Exercise 3.(10 marks) (a) Prove that there are no non-zero integers a, b such that $a^2=2b^2$. (Hint : Use the Fundamental Theorem of Arithmetic.)

(b) Show $\sqrt{2}$ is irrational. (Hint : Assume $\sqrt{2}=a/b$ where $a,\, b\in\mathbf{Z}$. Use (a) to derive a contradiction.)

Solution.(a) Set

$$m=a^2=2b^2.$$

We investigate the prime decomposition of m. If

$$a=p_1\cdots p_k$$

is the prime decomposition of a then the identity

$$m=a^2$$

yields that m has the prime decomposition

$$p_1\cdots p_k\cdot p_1\cdots p_k.$$

The preceding decomposition allows us to conclude that if p is a (positive) prime divisor of m then the number of occurences of p in the prime factorization of m must be even; in fact it is exactly twice the number of occurences of p in the factorization of a.

On the other hand, if

$$b=q_1\cdots q_l$$

is the prime factorization of b then the identity

$$m=2b^2$$

yields that m has the prime decomposition

$$2q_1\cdots q_l\cdot q_1\cdots q_l.$$

Each occurence of 2 in the prime decomposition of b thus contributes two occurences of 2 to that of m. Since there is an additonal occurence of 2 comming from factor 2, we deduce that 2 occurs an odd number of times in the prime factorization of m, a contradiction of the fact that each prime occurs an even number of times.

In light of the preceding discussion, we deduce that there are no non-zero integers a and b for which $a^2=2b^2$.

(b) If $\sqrt{2}$ where rational then there would exist non-zero integers a and b such that

$$\sqrt{2}=\frac{a}{b}.$$

Squaring both sides and clearing denominators, we deduce

$$2b^2=a^2$$

for non-zero integers. Since this contadicts part (a), we deduce $\sqrt{2}$ is irrational.

Exericse 4.(10 marks) Prove the following identities.

(a) If n is a positive integer then

$$1 + 3 + \cdots + (2n - 1) = n^2.$$

(b) Let $r \neq 1$ be a real number. If n is a positive integer then

$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}.$$

Solution. (a) If $n = 1$ then

$$1 = 1^2.$$

Let $k \geq 1$ and assume

$$1 + \cdots + (2k - 1) = k^2.$$

We calculate

$$\begin{aligned} 1 + \cdots + (2k-1) + (2(k+1) - 1) &= [1 + \cdots + (2k-1)] + 2k + 1 \\ &= k^2 + 2k + 1 = (k+1)^2. \end{aligned}$$

(PMI) allows us to conclude

$$1 + \cdots + (2n - 1) = n^2$$

is true for all $n \geq 1$.

(b) If $n = 1$ then the identity

$$r^2 - 1 = (r - 1)(r + 1)$$

allows us to conclude

$$\frac{r^2 - 1}{r - 1} = 1 + r.$$

Let $k \geq 1$ and assume

$$1 + r + \cdots + r^k = \frac{r^{k+1} - 1}{r - 1}.$$

We calculate

$$\begin{aligned} 1 + r + \cdots + r^k + r^{k+1} &= \left[1 + r + \cdots + r^k\right] + r^{k+1} \\ &= \frac{r^{k+1} - 1}{r - 1} + r^{k+1} \\ &= \frac{r^{k+1} - 1 + r^{k+1}(r - 1)}{r - 1} \\ &= \frac{r^{k+2} - 1}{r - 1}. \end{aligned}$$

(PMI) allows us to conclude

$$1 + r + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

is true for all $n \geq 1$.

Exercise 5.(15 marks) Let $(F_n) = (1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots)$be the Fibonacci sequence defined by

$$F_1 = F_2 = 1, \qquad F_n = F_{n-1} + F_{n-2} \text{ if } n > 2.$$

Show that the following hold for $n \geq 1$.

(a) $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

(b) $F_1^2 + \cdots + F_n^2 = F_n F_{n+1}$.

(c) $F_n < (5/3)^n$.

Solution.(a) In the case $n = 1$,

$$F_1 = 1 = 2 - 1 = F_3 - 1 = F_{1+2} - 1.$$

Let $k \geq 1$ and assume

$$F_1 + \cdots + F_k = F_{k+2} - 1.$$

We calculate

$$\begin{aligned} F_1 + \cdots + F_k + F_{k+1} &= [F_1 + \cdots + F_k] + F_{k+1} \\ &= F_{k+2} - 1 + F_{k+1} \\ &= F_{k+2} + F_{k+1} - 1 = F_{k+3} - 1 = F_{k+1+2} - 1. \end{aligned}$$

(PMI) allows us to conclude

$$F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$$

for all $n \geq 1$.

(b) In the case $n = 1$,

$$F_1^2 = (1)^2 = 1 \cdot 1 = F_1 F_2.$$

Let $k \geq 1$ and assume

$$F_1^2 + \cdots + F_k^2 = F_k F_{k+1}.$$

We calculate

$$\begin{aligned} F_1^2 + \cdots + F_k^2 + F_{k+1}^2 &= \left[F_1^2 + \cdots + F_k^2\right] + F_{k+1}^2 \\ &= F_k F_{k+1} + F_{k+1}^2 \\ &= (F_k + F_{k+1}) F_{k+1} \\ &= F_{k+2} F_{k+1} = F_{k+1} F_{k+1+1}. \end{aligned}$$

(PMI) allows us to conclude

$$F_1^2 + \cdots + F_n^2 = F_n F_{n+1}$$

for all $n \geq 1$.

(c) We observe

$$F_1 = 1 < \frac{5}{3} \qquad \text{and} \qquad F_2 = 1 < 25/9 = \left(\frac{5}{3}\right)^2.$$

Let $k \geq 2$ and assume that

$$F_i < \left(\frac{5}{3}\right)^i$$

for $i = 1, 2, \ldots, k$. Using inductive definition of the Fibonacci sequence,

$$\begin{aligned} F_{k+1} = F_k + F_{k-1} &< \left(\frac{5}{3}\right)^k + \left(\frac{5}{3}\right)^{k-1} \\ &= \left(\frac{5}{3}\right)^{k-1} \left[\frac{5}{3} + 1\right] \\ &= \left(\frac{5}{3}\right)^{k-1} \cdot \frac{8}{3} \\ &< \left(\frac{5}{3}\right)^{k-1} \cdot \frac{25}{9} \\ &= \left(\frac{5}{3}\right)^{k-1} \left(\frac{5}{3}\right)^2 = \left(\frac{5}{3}\right)^{k+1}. \end{aligned}$$

(PCI) allows us to conclude

$$F_n < (5/3)^n$$

is true for all $n \geq 1$.

Exercise 6.(10 marks) (a) Show that 4 is a divisor of $7^n - 3^n$ for every positive integer n.
(b) Let $r > -1$ be a real number. Show that for every positive integer n, $(1+r)^n \geq 1 + rn$.
Solution. In the case $n = 1$,

$$7 - 3 = 4$$

is clearly divisible by 4. Let $k \geq 1$ and assume 4 divides $7^k - 3^k$. We note

$$7^{k+1} - 3^{k+1} = 7^{k+1} - 7 \cdot 3^k + 7 \cdot 3^k - 3^{k+1} = 7 \cdot (7^k - 3^k) + (7-3) \cdot 3^k = 7 \cdot (7^k - 3^k) + 4 \cdot 3^k.$$

By assumption, there exists an integer q such that $7^k - 3^k = 4q$, hence the preceding calculation yields

$$7^{k+1} - 3^{k+1} = 7 \cdot 4q + 4 \cdot 3^k = 4(7q + 3^k),$$

i.e. $4 | 7^{k+1} - 3^{k+1}$.

(PMI) allows to conclude 4 divides the difference $7^n - 3^n$ for all $n \geq 1$.

(b) When $n = 1$,

$$(1+r)^1 = 1 + r.$$

Let $k \geq 1$ and assume $(1+r)^k \geq 1 + rk$. Observing that the assumption $r > -1$ ensures that $1 + r > 0$, we calculate

$$\begin{aligned}(1+r)^{k+1} = (1+r)^k(1+r) &\geq (1+rk)(1+r)\\ &= 1 + rk + r + r^2k\\ &= 1 + r(k+1) + r^2k\\ &\geq 1 + r(k+1),\end{aligned}$$

since $r^2k \geq 0$. (PMI) allows us to conclude that if $r \geq -1$ then $(1+r)^n \geq 1 + rn$ for all $n \geq 1$.