Homework #2. Due Thursday, January 29th, in class

Reading:

1. For this assignment: Section 2.2, 2.3 and parts of 2.4 (greatest common divisor) + class notes (Lectures 3-4).
2. For next week's classes: the rest of 2.4 (primes and factorization) and 2.5 (start).

Problems:

Problem 1: Consider the following "proof" by induction: For each $n \in \mathbb{N}$ let $P(n)$ be the statement

$$\sum_{i=0}^{n} 2^i = 2^{n+1}. \qquad (***)$$

Claim: $P(n)$ is true for all $n \in \mathbb{N}$.

Proof: "$P(n-1) \Rightarrow P(n)$." Assume that $P(n-1)$ is true for some $n \in \mathbb{N}$. Then $\sum_{i=0}^{n-1} 2^i = 2^n$. Adding 2^n to both sides, we get $\sum_{i=0}^{n-1} 2^i + 2^n = 2^n + 2^n$, whence $\sum_{i=0}^{n} 2^i = 2^{n+1}$, which is precisely $P(n)$. Thus, $P(n)$ is true.

By the principle of mathematical induction, $P(n)$ is true for all n. $\square$

(a) Show that the statement $P(n)$ is false (it is actually false for any n).

(b) Explain why the above "proof" does not contradict the principle of mathematical induction, that is, find a mistake in the above "proof" (Hint: the mistake is in the general logic).

Problem 2: Recall that in Lecture 3 we proved that for every $n \in \mathbb{N}$ there exist $a_n, b_n \in \mathbb{Z}$ such that $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$. Moreover, we showed that such a_n and b_n satisfy the following recursive relations: $a_1 = b_1 = 1$ and $a_{n+1} = a_n + 2b_n$, $b_{n+1} = a_n + b_n$ for all $n \in \mathbb{N}$.

(a) Use the above recursive formulas and mathematical induction to prove that $a_n^2 - 2b_n^2 = (-1)^n$ for all $n \in \mathbb{N}$.

(b) Prove that for all $n \in \mathbb{N}$ there exist $c_n, d_n \in \mathbb{Z}$ such that $(1+\sqrt{3})^n = c_n + d_n\sqrt{3}$.

(c) (bonus) Find a simple formula relating c_n and d_n (similar to the one in (a)) and prove it.

Problem 3: Let $a, b, c \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$. Prove directly from definition of divisibility that $c \mid (ma + nb)$ for any $m, n \in \mathbb{Z}$ (do not refer to any divisibility properties proved in class).

Problem 4: Let $a, b, c \in \mathbb{Z}$ such that $c \mid ab$. Is it always true that $c \mid a$ or $c \mid b$? If the statement is true for all possible values of a, b, c, prove it; otherwise give a counterexample.

Problem 5: Let $a = 382$ and $b = 26$. Use Euclidean algorithm to compute $gcd(a, b)$ and find $u, v \in \mathbb{Z}$ such that $au + bv = gcd(a, b)$.

Problem 6: Prove the key lemma, justifying the Euclidean algorithm:

Lemma: Let $a, b \in \mathbb{Z}$ with $b > 0$. Divide a by b with remainder: $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.

Hint: Show that the pairs $\{a, b\}$ and $\{b, r\}$ have the same set of common divisors, that is,

(i) if $c \mid a$ and $c \mid b$, then $c \mid r$ (and so c divides both b and r)
(ii) if $c \mid b$ and $c \mid r$, then $c \mid a$ (and so c divides both a and b).

Problem 7: Let $a, b \in \mathbb{Z}$, not both 0, let $d = \gcd(a, b)$, and let

$$S = \{x \in \mathbb{Z} : x = am + bn \text{ for some } m, n \in \mathbb{Z}\}.$$

By GCD Theorem, d is the smallest positive element of S, and a natural problem is to describe all elements of S.

(a) Prove that if k is any element of S, then $d \mid k$. **Hint:** Problem 3.
(b) Prove that if $k \in \mathbb{Z}$ and $d \mid k$, then $k \in S$. **Hint:** Use the first of part of GCD Theorem (as stated in class).
(c) Deduce from (a) and (b) that elements of S are precisely integer multiples of d.

Problem 8: Given $n, k \in \mathbb{Z}$ with $0 \leq k \leq n$, define the binomial coefficient $\binom{n}{k}$ by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

(recall that $0! = 1$).

(a) Prove that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ for any $1 \leq k < n$ (direct computation).
(b) Now prove the binomial theorem: for every $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \ldots + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n.$$

Hint: Use induction on n. For the induction step write $(a + b)^n = (a + b)^{n-1} \cdot (a + b)$ and use part (a).