PROBLEM FROM LOVASZ’S BOOK: INTEGERS

(1) Assume that $a|b$, and $a, b > 0$. Let $r$ be the remainder of the division $c \div a$, and let $s$ be the remainder of the division $c \div b$. What is the remainder of the division $s \div a$?

(2) (a) Prove that for every integer $a$, $a - 1|a^2 - 1$.
(b) More generally, for every integer $a$ and positive integer $n$, $a - 1|a^n - 1$.

(3) (a) Show that $\sqrt{2}$ is irrational.
(b) More generally, show that $\sqrt{p}$, for any prime $p$, is irrational.

(4) (a) Prove that if $p$ is a prime, and $a$ and $b$ are integers, and $p|ab$, then either $p|a$ or $p|b$ (or both).
(b) Suppose that $a$ and $b$ are integers and $a|b$. Also suppose that $p$ is a prime and $p|b$ but $p \not| a$. Show that $p$ is a divisor of the ratio $b/a$.

(5) (b) More generally, show that $\sqrt{p}$, for any prime $p$, is irrational.

(6) Are there any even primes?

(7) Prove that if $p$ is a prime, then $\sqrt{2}$ is irrational. More generally, prove that if $n$ is an integer that is not a square, the $\sqrt{n}$ is irrational.

(8) For every positive integer $k$, there exist $k$ consecutive composite integers.

(9) If $p$ is a prime and $0 < k < p$, then $p|\binom{p}{k}$.

Hints: We can write $\binom{p}{k} = \frac{p(p-1)...(p-k+1)}{k(k-1)(k-2)...1}$. Since $p$ is a prime greater than $k$, $p$ does not divide the denominator.

Show by an example that this assertion is not true if $p$ is not a prime number.

(10) Fermat’s Little Theorem: If $p$ is a prime and $a$ is an integer, the $p|a^p - a$.

Proof: Can be proved using induction on $a$. Let $S(a)$ be the proposition that “$p|a^p - a$”. Clearly $S(1)$ is true. Suppose $S(1) \land S(k)$ is true. Now

$$(k + 1)^p - (k + 1) = k^p + \binom{p}{1}k^{p-1} + ... + \binom{p}{p-1}k + 1 - (k + 1)$$

$$= (k^p - k) + \binom{p}{1}k^{p-1} + ... + \binom{p}{p-1}k.$$ 

$p$ divides $k^p - k$ since $S(k)$ is true. The other terms are also divisible by $p$. Therefore $S(k+1)$ is true. Therefore, $S(a)$ is true for all $a$ (by the principle of induction).

(11) (a) If $a$ is even and $b$ is odd, $\gcd(a, b) = \gcd(a/2, b)$.
(b) If both $a$ and $b$ are even, $\gcd(a, b) = 2\gcd(a/2, b/2)$. 
(12) How can you express the least common multiple of two integers if you know the prime factorization of each?

(13) Suppose that you are given two integers, and you know the prime factorization of one of them. Describe a way of computing the greatest common divisor of these numbers.

(14) Prove that for any two integers $a$ and $b$, $\gcd(a, b) \times \text{lcm}(a, b) = a \times b$.

(15) Show that the Euclidean Algorithm can terminate in two steps for arbitrarily large positive integers, even if their g.c.d. is 1.

(16) Describe the Euclidean Algorithm applied to two consecutive Fibonacci numbers. Use your description to show that the Euclidean Algorithm can take arbitrarily many steps.

(17) Consider the following version of the Euclidean algorithm to compute $\gcd(a, b)$:

1. Swap the numbers necessary to have $a \leq b$;
2. If $a = 0$, return $b$;
3. if $a \neq 0$, then replace $b$ by $b - 1$ and go to (1).

- Carry out this algorithm to compute $\gcd(19, 2)$.
- Show that the modified Euclidean Algorithm always terminates with the correct answer.
- How long does this algorithm take, in the worst case, when applied to two 100-digit integers?