Homework 2, solutions

Problem 1. Suppose that $a_1 = 2$ and $a_{n+1} = 3a_n + 2$. Prove that $a_n = 3^n - 1$ for every natural number n.

Solution: Let $P(n)$ be the statement:

$$a_n = 3^n - 1.$$

We prove that $P(n)$ is true for all $n \geq 1$ by induction on n.

First we check $P(1)$: $a_1 = 2 = 3^1 - 1$, so $P(1)$ is true.

Now we do the inductive step. Assume that $n \geq 1$ and $P(1), P(2), \ldots, P(n)$ are true. We need to show that $P(n+1)$ is also true. Since $P(n)$ is true, we know that $a_n = 3^n - 1$. It follows that

$$a_{n+1} = 3a_n + 2 = 3(3^n - 1) + 2 = 3^{n+1} - 1.$$

Thus $P(n+1)$ is true. The method of mathematical induction tells us that $P(n)$ is true for every $n \geq 1$.

Problem 2. Let $F_n = 2^{2^n} + 1$, for $n = 0, 1, 2, ...$

a) Prove that $F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_n = F_{n+1} - 2$ for every n.

b) Prove that $\gcd(F_n, F_m) = 1$ for $n \neq m$.

c) Use b) to give yet another proof that the set of primes is infinite.

Solution: a) The easiest proof seems to be by induction on n. Let $P(n)$ be the statement

$$F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_n = F_{n+1} - 2.$$

Since $F_0 = 3 = 5 - 2 = F_1 - 2$, we see that $P(0)$ is true.

Suppose now that $n \geq 0$ and $P(0), \ldots, P(n)$ are true. In particular, $P(n)$ is true, so

$$F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_n = F_{n+1} - 2 = 2^{2^{n+1}} - 1.$$

Multiplying both sides by $F_{n+1} = 2^{2^{n+1}} + 1$ we get

$$F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_n \cdot F_{n+1} = (2^{2^{n+1}} - 1)(2^{2^{n+1}} + 1) = 2^{2^{n+2}} - 1 = F_{n+2} - 2.$$

so $P(n+1)$ is true. By induction, $P(n)$ is true for every $n \geq 0$.

b) Suppose that $m < n$ and d is the greatest common divisor of F_m and F_n. Clearly d divides $F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_{n-1}$ (since F_m is one of the factors) and therefore it divides the difference $F_n - F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_{n-1}$, which is 2 by a). Thus $d|2$, i.e. $d = 1$ or $d = 2$. Hovewer $d = 2$ is not possible, since the numbers F_k are all odd. Hence $d = 1$, i.e. $\gcd(F_n, F_m) = 1$.

c) Each of the numbers F_n has a prime divisor, call it p_n. Since any two among the numbers F_n are relatively prime, no two of the primes p_n can be the same. Thus we have an infinite list of pairwise distinct prime numbers.

Remark. The numbers F_n are called **Fermat's numbers**. It is no hard to see that F_0, F_1, F_2, F_3, F_4 are prime numbers. However, Euler proved that F_5 is not a prime. It is still unknown if there exists $n > 4$ such that F_n is a prime number.

Problem 3. Read the proof of Proposition 1.22 (page 32) in the book (we went over it in clas). Using simialr method prove that there are infinitely many prime numbers of the form $3n + 2$.

Solution. Note that every prime number different from 3 is either of the form $3k+1$ or of the form $3k + 2$. Note also that a product of any 2 numbers of the form $3k + 1$ is again of this form:

$$(3a + 1)(3b + 1) = 3(3ab + a + b) + 1.$$

It follows that any positive integer n of the form $3k + 2$ must have a prime divisor of the form $3k + 2$. Indeed, otherwise all prime divisors of n would be of the form $3k + 1$ (note that $3 \nmid n$) and n would be a product of these primes, hence it would again be of the form $3k + 1$.

Now we can follow Euclid's proof that the set of all primes is infinite. Suppose that $p_1, \ldots, p_m$ are odd primes of the form $3k + 2$. Consider the number $N = 3p_1p_2 \ldots p_m + 2$. As we noticed above, N must have a prime divisor p of the form $3k + 2$ and this divisor must be odd, as N is odd. But none of the odd primes $p_1, \ldots, p_m$ can divide N (as they all divide $N - 2$) so p must be a new odd prime of the form $3k + 2$.

Remark. Alternatively, one could look at $n! - 1$, which is of the form $3k + 2$ for $n \geq 3$, and conclude that it must have a prime divisor of the form $3k + 2$ and any such divisor is bigger than n.

Problem 4. Recall that when p is a prime number and $n \neq 0$ an integer then $e_p(n)$ is the largest integer a such that $p^a | n$.

a) Prove that if $n > 1$ and $p > n$ is a prime then $e_p(n!) = 0$

b) Recall thal $\lfloor x \rfloor$ denotes the largest integer not exceeding x. Prove that if n, k are positive integers then

$$\left\lfloor \frac{n+1}{k} \right\rfloor = \begin{cases} \lfloor \frac{n}{k} \rfloor & \text{if } k \nmid (n+1) \\ 1 + \lfloor \frac{n}{k} \rfloor & \text{if } k | (n+1) \end{cases}.$$

c) Prove that if $n > 1$ and $p \leq n$ is a prime then

$$e_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

(note that the sum is actually finite since $\lfloor n/p^k \rfloor = 0$ when $p^k > n$.

Hint. There are several ways to prove this, but I suggest a proof by induction on n. Note that $e_p((n+1)!) = e_p(n!) + e_p(n+1)$ and use part b) (this is why b) is part of this problem).

d) Use c) to write the prime factorization of 20!.

e) Find the number of zeros with which the decimal representation of 99! terminates.

Solution. a) Note that if $p > k > 0$ then $e_p(k) = 0$. Recall that $e_p(ab) = e_p(a) + e_p(b)$. It follows that

$$e_p(n!) = e_p(2) + e_p(3) + \dots + e_p(n) = 0$$

when $p > n$.

b) Let $m = \lfloor n/k \rfloor$. Then $m \leq n/k < (m+1)$, so $km \leq n < k(m+1)$. It follows that $km < n+1 \leq k(m+1)$ (we are using here a simple but very useful observation that if $a < b$ are integers then $a + 1 \leq b$). If $k \nmid (n+1)$, then we cannot have equality on

the right, i.e. $km < n+1 < k(m+1)$. This means that $m < (n+1)/k < (m+1)$, i.e $m = \lfloor (n+1)/k \rfloor$. On the other hand, if $k|(n+1)$ then from $km < n+1 \leq k(m+1)$ we conclude that $n+1 = k(m+1)$, so $m+1 = (n+1)/k = \lfloor (n+1)/k \rfloor$.

c) First note that we do not need to assume that $p \leq n$ as for $p > n$ the right hand side of the formula is clearly 0 and the left hand side is also 0 by part a).

We use induction on n. Let $P(n)$ be the following statement:

$$e_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots \quad \text{for all prime numbers } p.$$

For $n = 2$ we already now that the formula works when $p > 2$ and for $p = 2$ it clearly works as well:

$$e_2(2!) = 1 = \left\lfloor \frac{2}{2} \right\rfloor + \left\lfloor \frac{2}{2^2} \right\rfloor + \left\lfloor \frac{2}{2^3} \right\rfloor + \dots .$$

Thus $P(2)$ is true.

Suppose that $n \geq 2$ and $P(2), \dots, P(n)$ are true. We want to show $P(n+1)$ is true. Consider a prime number p. So we know that

$$e_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots .$$

Let $e_p(n+1) = k$. Then $p^i | n+1$ for $i \leq k$ and $p^i \nmid n+1$ for $i > k$. By part b) we have

$$\left\lfloor \frac{n+1}{p^i} \right\rfloor = \begin{cases} \left\lfloor \frac{n}{p^i} \right\rfloor & \text{if } i > k \\ 1 + \left\lfloor \frac{n}{p^i} \right\rfloor & \text{if } i \leq k \end{cases}.$$

It follows that

$$\left\lfloor \frac{n+1}{p} \right\rfloor + \left\lfloor \frac{n+1}{p^2} \right\rfloor + \left\lfloor \frac{n+1}{p^3} \right\rfloor + \dots = k + \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots =$$
$$e_p(n+1) + e_p(n!) = e_p((n+1)!).$$

Thus $P(n+1)$ holds. By the method of induction, the formula is true for all prime numbers p and all integers $n \geq 2$.

d) By a), we know that only primes smaller than 20 will contribute to 20!. Now we use our formula from c) to compute the contributions of the primes up to 20:

$$e_2(20!) = \left\lfloor \frac{20}{2} \right\rfloor + \left\lfloor \frac{20}{4} \right\rfloor + \left\lfloor \frac{20}{8} \right\rfloor + \left\lfloor \frac{20}{16} \right\rfloor = 10 + 5 + 2 + 1 = 18.$$

$$e_3(20!) = \left\lfloor \frac{20}{3} \right\rfloor + \left\lfloor \frac{20}{9} \right\rfloor = 6 + 2 = 8.$$

$$e_5(20!) = \left\lfloor \frac{20}{5} \right\rfloor = 4.$$

$$e_7(20!) = \left\lfloor \frac{20}{7} \right\rfloor = 2.$$

$$e_{11}(20!) = \left\lfloor \frac{20}{11} \right\rfloor = 1.$$

$$e_{13}(20!) = \left\lfloor \frac{20}{13} \right\rfloor = 1.$$

$$e_{17}(20!) = \left\lfloor \frac{20}{17} \right\rfloor = 1.$$

$$e_{19}(20!) = \left\lfloor \frac{20}{19} \right\rfloor = 1.$$

Thus $20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

e) Note that the number of zeros with which the decimal representation of some nunber n terminates is euqal to the highest power of 10 which divides n. Since $10 = 2 \cdot 5$, the highest power of 10 dividing n is equal to the smaller of the numbers $e_2(n)$ and $e_5(n)$.

Now, by part c), we have

$$e_2(99!) = \left\lfloor \frac{99}{2} \right\rfloor + \left\lfloor \frac{99}{4} \right\rfloor + \left\lfloor \frac{99}{8} \right\rfloor + \left\lfloor \frac{99}{16} \right\rfloor + \left\lfloor \frac{99}{32} \right\rfloor + \left\lfloor \frac{99}{64} \right\rfloor = 49+24+12+6+3+1 = 95$$

and

$$e_5(99!) = \left\lfloor \frac{99}{5} \right\rfloor + \left\lfloor \frac{99}{25} \right\rfloor = 19 + 3 = 22.$$

Thus 99! ends with 22 zeros.

Problem 5. a) Prove that if a, b, c are integers and $\gcd(a, c) = 1 = \gcd(b, c)$ then $\gcd(ab, c) = 1$.

b) Prove that if $\gcd(a, b) = 1$ then $\gcd(a^n, b^m) = 1$ for all positive integers m, n.

c) Prove that if $\gcd(a^n, b^m) = 1$ for some positive integers m, n then $\gcd(a, b) = 1$.

d) Prove that if n is a positive integer and $a^n | b^n$ then $a | b$.

Solution. a) Suppose that a prime p divides both ab and c. Then, by Euclid's Lemma, p divides either a or b. This however is not possible, as both $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$. Thus ab and c cannot have any common prime divisors, hence $\gcd(ab, c) = 1$.

b) Suppose that a prime p divides both a^n and b^m. By Euclid's Lemma, p divides a and p divides b. This however contradicts our assumption that $\gcd(a, b) = 1$. Thus a^n, b^m cannot have any common prime divisors, hence $\gcd(a^n, b^m) = 1$.

c) If $d|a$ and $d|b$ then $d|a^n$ and $d|b^m$ so $d = 1$, as $\gcd(a^n, b^m) = 1$. Thus $\gcd(a, b) = 1$.

d) Let $d = \gcd(a, b)$ so $a = da_1$, $b = db_1$ and $\gcd(a_1, b_1) = 1$. Since $(da_1)^n|(db_1)^n$, we have $a_1^n|b_1^n$. However, $\gcd(a_1^n, b_1^n) = 1$ by part b). Thus $a_1^n = 1$, so $a_1 = 1$ and $d = a$. It follows that $a|b$.