Homework 3, solutions

Problem 1. Read the proof of Proposition 1.22 (page 32) in the book. 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 2. Let $a > 1$ and $n > 1$ be positive integers.

a) Prove that if $a^n - 1$ is a prime then $a = 2$ and n is a prime.

b) Prove that if $a^n + 1$ is a prime then a is even and $n = 2^k$ for some k (Hint: if n is not a power of 2 then n has an odd divisor).

Hint. The identity $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + ab^{n-2} + b^{n-1})$ should be helpful. Prove this identity.

Solution. a) Recall that we proved that $a^n - 1 = (a-1)(1 + a + a^2 + \ldots + a^{n-1})$.

If $a > 2$ then this identity provides a factorization of $a^n - 1$ into two factors bigger than 1, hence $a^n - 1$ cannot be a prime number. Suppose now that $a = 2$. If n is not a prime, then $n = kl$ for some integers $k > 1$, $l > 1$. Note that $a^n = (a^l)^k$ and our identity yields

$$a^n - 1 = (a^l)^k - 1 = (a^l - 1)(1 + a^l + (a^l)^2 + \ldots + (a^l)^{n-1})$$

so $a^n - 1$ is not a prime.

Thus when $a^n - 1$ is a prime we must have $a = 2$ and n has to be a prime.

b) The resoning here is similar to the one in a) but it is based on the identity

$$a^n + 1 = (a + 1)(1 - a + a^2 - \ldots + a^{n-1}),$$

which holds for all **odd** natural numbers n. This identity follows from the identity used in a) by observing that for n odd we have

$$a^n + 1 = -((-a)^n - 1) = -((-a) - 1)(1 + (-a) + (-a)^2 + \ldots + (-a)^{n-1}) =$$

$$(a + 1)(1 - a + a^2 - \ldots + a^{n-1}.$$

Suppose now that n is not a power of 2. Then $n = kl$ for some odd $k > 1$. Thus

$$a^n + 1 = (a^l)^k + 1 = (a^l + 1)(1 - a^l + (a^l)^2 - \ldots + (a^l)^{k-1})$$

i.e. $a^n + 1$ factors into a product of two integers bigger than 1. Thus $a^n + 1$ cannot be a prime. In other words, if $a^n + 1$ is a prime, then n must be a power of 2. Moreover, as $a^n + 1 > 2$, $a^n + 1$ must be odd, hence a must be even.

Remark. The identity in the hint follows from the identity used in a). We have

$$\left(\frac{a}{b}\right)^n - 1 = \left(\frac{a}{b} - 1\right)\left(1 + \left(\frac{a}{b}\right) + \left(\frac{a}{b}\right)^2 + \ldots + \left(\frac{a}{b}\right)^{n-1}\right).$$

Multiply both sides by b^n to get the identity in the hint.

Problem 3. 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

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

(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

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

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

Suppose that the formula works for all primes and numbers $n = 2, 3, \dots N$. We want to show that it works when $n = N + 1$. 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 the formula indeed works for $N + 1$. 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 4. 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 $(da_1)^n|(db_1)^n$ then $a_1^n|b_1^n$. 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 $a|b$.