

Solutions to Problem Set VII

NUMBER THEORY AND ARITHMETIC

- (a) If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the prime factorization of $n \geq 2$ as in above, find a formula for the number of divisors of n . (*Hint:* First try it for simpler cases when $n = p^a$ has only one prime divisor or $n = p^a q^b$ has two prime divisors and then generalize that.)
(b) An even number is divisible by 5 and has 35 divisors. What it can be?

Solution:

- (a) One can see that the divisors are integers like $d = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where for each $1 \leq i \leq k$, we have $0 \leq b_i \leq a_i$. Therefore, we have $a_i + 1$ options for each number b_i : all the numbers $\{0, 1, \dots, a_i\}$. So, for constructing a divisor of n , we have $a_1 + 1$ options for the first power, $a_2 + 1$ options for the second power and so on. Therefore, over all we have $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$ divisors for n .
(b) If n is such a number, we know that it is divisible by 2 and 5. Therefore, we can assume that its factorization is $n = 2^r \cdot 5^s \cdot p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where r and s are positive integers and p_i are primes other than 2 and 5. The first part of this problem shows that number of divisors of n is $(r + 1)(s + 1)(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$, where $r + 1$ and $s + 1$ are integers bigger than one. But, we know this number is 35 and there is only two ways to write 35 as product of numbers bigger than one: 5×7 or 7×5 . Therefore, either $r + 1 = 5$ and $s + 1 = 7$ or $r + 1 = 7$ and $s + 1 = 5$ and in either case n cannot have any other prime divisors. Therefore the only possibilities for n is: $n = 2^4 \times 5^6$ or $n = 2^6 \times 5^4$.
- (a) Let n be an integer which is not divisible by any integer $2 \leq k \leq \sqrt{n}$. Prove that n is prime.
(b) If p is a prime prove that $p \mid \binom{p}{k}$, whenever $0 < k < p$.
(c) Prove that $p \mid n^p - n$, for any $n \in \mathbb{N}$.

Solution:

- (a) If n is not a prime, it has a divisor d which is different from n and 1: $1 < d < n$. Also, there exists an integer k such that $dk = n$ and we have $1 < k < n$ as well. But, k and d both cannot be bigger than \sqrt{n} ; otherwise $n = dk > \sqrt{n} \cdot \sqrt{n} = n$, which is impossible. Therefore one of d and k is bigger than 1 and less than or equal to \sqrt{n} .
(b) $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. In other terms,

$$p! = \binom{p}{k} \cdot k! \cdot (p - k)!$$

The left side of the above equation is divisible by p , so should be the right side. But since $0 < k < p$, neither $k!$ nor $(p - k)!$ is divisible by p and we have to have $p \mid \binom{p}{k}$.

- (c) We prove this part by induction on n . For $n = 1$, the statement is obvious. Now assume we know that $p \mid n^p - n$ and we want to prove the statement for $n + 1$: $p \mid (n + 1)^p - (n + 1)$. First note that by binomial theorem:

$$(n + 1)^p = n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \cdots + \binom{p}{p-1}n + 1.$$

Because of part (b), all the summands of the above sum are divisible by p except for the first and last ones. But by induction hypothesis, we also know that $n^p - n$ is divisible by p . Therefore if we subtract $n + 1$ from the above sum it will be divisible by p and this proves that $p \mid (n + 1)^p - (n + 1)$ and we have finished the proof.

3. For integers a and b show the following:

- (a) $\gcd(a, b) = \gcd(a, a - b)$,
 (b) if $0 \leq r < b$ is the remainder of a when divided by b prove that $\gcd(a, b) = \gcd(b, r)$,
 (c) prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for any $n \in \mathbb{N}$.

Solution:

- (a) If $d = \gcd(a, b)$ then $d \mid a$ and $d \mid b$. Therefore, $d \mid a - b$. Since d divides both a and $a - b$, it should be less than or equal to $\gcd(a, a - b)$. On the other hand if $k = \gcd(a, a - b)$, $k \mid a$ and $k \mid a - b$. Therefore, k divides $a - (a - b) = b$. So k divides both a and b and it has to be less than or equal to $\gcd(a, b)$. For $\gcd(a, b)$ and $\gcd(a, a - b)$, I have proved that each is less than or equal to the other one. This is impossible, unless $\gcd(a, b) = \gcd(a, a - b)$.
- (b) If r is the remainder of a when divided by b it means that, there exists an integer q , such that $a = qb + r$ or $r = a - qb$. Part (a) above shows that $\gcd(a, b) = \gcd(a, a - b)$. Also $\gcd(a, b) = \gcd(a - b, b)$. If we use this again for $\gcd(b, a - b)$, we see that $\gcd(a - b, b) = \gcd(a - 2b, b)$. We can continue this q times and we have:

$$\begin{aligned} \gcd(a, b) &= \gcd(a - b, b) = \gcd(a - 2b, b) = \gcd(a - 3b, b) = \cdots = \gcd(a - qb, b) \\ &\Rightarrow \gcd(a, b) = \gcd(r, b). \end{aligned}$$

Note: In the earlier version, I had a misprint stating that $\gcd(a, b) = \gcd(a, r)$. This is wrong in general and you could give a counter example. For example, if $a = 14$ and $b = 5$, $\gcd(14, 5) = 1$; but the remainder of 14 when divided by 5 is 4 and we have $\gcd(14, 4) = 2 \neq 1$.

- (c) To show that this is irreducible, we need to show that $\gcd(21n + 4, 14n + 3) = 1$. Using part (a) a few times gives:

$$\begin{aligned} \gcd(21n + 4, 14n + 3) &= \gcd((21n + 4) - (14n + 3), 14n + 3) = \gcd(7n + 1, 14n + 3) \\ &= \gcd(7n + 1, (14n + 3) - (7n + 1)) = \gcd(7n + 1, 7n + 2) \\ &= \gcd(7n + 1, (7n + 2) - (7n + 1)) = \gcd(7n + 1, 1) \\ &= 1. \end{aligned}$$

4. If $\gcd(a, b) = 1$, prove that

- (a) $\gcd(a - b, a + b) \leq 2$,
- (b) $\gcd(a - b, a + b, ab) = 1$,
- (c) $\gcd(a^2 - ab + b^2, a + b) \leq 3$.

Solution:

- (a) If something divides both $a+b$ and $a-b$ it will divide $(a+b)+(a-b)$ and $(a+b)-(a-b)$ as well. But, these are $2a$ and $2b$. But the only common divisor of $2a$ and $2b$ can be 2, because a and b are relatively prime. Therefore $\gcd(a-b, a+b)$ cannot be bigger than 2.
- (b) Above we showed that $\gcd(a - b, a + b)$ is either 1 or 2. If it is 1 then of course $\gcd(a - b, a + b, ab) = 1$ too. Otherwise, 2 divides both $a - b$ and $a + b$. Therefore, a and b are either both even or odd. They cannot be even at the same time, since then $2|a$ and $2|b$ and they wouldn't be relatively prime. So, they are both odd and ab is odd too. So the only nontrivial common divisor of $a - b$ and $a + b$, 2, is not a divisor of ab and therefore $\gcd(a - b, a + b, ab) = 1$.
- (c) If $d = \gcd(a^2 - ab + b^2, a + b) \leq 3$, then $d|a + b$. We claim that d and ab are relatively prime. For that we just need to show that they don't have any common prime factor. If $p|ab$ is a prime, then either $p|a$ or $p|b$. If also $p|a + b$ then it has to divide both of them and it is impossible since $\gcd(a, b) = 1$. Now we observe that $a^2 - ab + b^2 = (a + b)^2 - 3ab$. d divides $a + b$, thus it divides $(a + b)^2$. It also divides $a^2 - ab + b^2 = (a + b)^2 - 3ab$, so it divides $3ab$. But, we saw that d and ab are relatively prime and therefore $d|3$ and this proves the statement.