Solutions to Problem Set VIII

More on Number Theory

Due Mar. 25th

1. Let n be a positive integer such that $n+1$ is divisible by 24. Prove that the sum of all the divisors of n is divisible by 24.

   Solution: We have $n \equiv -1 (\text{mod } 24)$. If $d|n$, there exists k such that $dk = n$ and $k|n$ also. Since n is relatively prime to 24, so are d and k. Therefore, modulo 24, d and k are congruent to one of the numbers 1, 5, 7, 11, $-11, -7, -5, -1$. But, we have $dk = n \equiv -1 (\text{mod } 24)$ and for any two number a and b in $1, 5, 7, 11, -11, -7, -5, -1$, it is easy to verify that $ab \equiv -1 (\text{mod } 24)$ if and only if $a = -b$. Therefore, $d \equiv -k (\text{mod } 24)$ and $d + k$ is divisible by 24 and of course they are distinct. So, the divisors come in pairs whose sum is divisible by 24 and thus the sum of all divisors is divisible by 24.

2. Prove that any two consecutive Fibonacci numbers F_n, F_{n+1}, $n > 2$, are relatively prime, i.e. $\gcd(F_n, F_{n+1}) = 1$. The Fibonacci numbers are defined recursively by:

   $$F_0 = 1,\ F_1 = 1 \quad \text{and} \quad F_{n+2} = F_{n+1} + F_n \quad \text{for } n \geq 0.$$

   Solution: In one of the homeworks in the last set, we showed that $\gcd(a, b) = \gcd(a-b, b)$. (It is in fact an easy exercise!) In particular,

   $$\gcd(F_{n+1}, F_n) = \gcd(F_{n+1} - F_n, F_n) = \gcd(F_{n-1}, F_n).$$

   We use induction. For $n = 0$, we have $\gcd(F_0, F_1) = \gcd(1, 1) = 1$ and the above fact shows how one can imply the statement for n by having it for $n - 1$.

3. (a) If $x^3 + y^3 = z^3$ has a solution in integers x, y, z, show that one of the three must be a multiple of 7.

   (b) If n is a positive integer greater than 1 such that $2^n + n^2$ is prime, show that $n \equiv 3 (\text{mod } 6)$.

   Solution:

   (a) Any integer x is congruent to one of the numbers $\pm 1, \pm 2$ or ± 3 modulo 7. One can see that in any case x^3 will be congruent to either 1 or -1. Therefore, either x^3 and y^3 are congruent with each other and to either 1 or -1 modulo 7 or $x^3 \equiv -y^3 (\text{mod } 7)$. In the former case, $x^3 + y^3 \equiv \pm 2 (\text{mod } 7)$ cannot be z^3 for any integer z and in the latter case, $z^3 = x^3 + y^3 \equiv 0 (\text{mod } 7)$ will be divisible by 7.

(b) It is easy to see that $2^n \equiv 2 (\mathrm{mod}\ 6)$ when n is odd. If $n \equiv \pm 1 (\mathrm{mod}\ 6)$ then n is odd, $n^2 \equiv 1 (\mathrm{mod}\ 6)$ and therefore $2^n + n^2 \equiv 2 + 1 = 3 (\mathrm{mod}\ 6)$ is divisible by 3 and is not a prime and if $n \equiv \pm 2 (\mathrm{mod}\ 6)$ then of course n is even and $n^2 + 2^n$ is also even and cannot be prime either. So, the only left possibility is than $n \equiv 3 (\mathrm{mod}\ 6)$.

4. (a) Prove that if one of the numbers $2^n - 1$ and $2^n + 1$ is prime, $n > 2$, then the other number is not.

   (b) What is the largest number N for which you can say that $n^5 - 5n^3 + 4n$ is divisible by N for every integer n?

   Solution:

   (a) The numbers $2^n - 1, 2^n$ and $2^n + 1$ are consecutive, therefore one of them is divisible by 3. But 2^n is not divisible by 3 and therefore one of the other two is and it cannot be a prime.

   (b) $n^5 - 5n^3 + 4n = (n-2)(n-1)n(n+1)(n+2)$ is the product of 5 consecutive integers and therefore is divisible by 5!. We proved this in general in class. So $n^5 - 5n^3 + 4n$ is always divisible by 5!. On the other hand, for $n = 3$, $n^5 - 5n^3 + 4n = 5!$ cannot be divisible by anything larger.

5. Given an integer n, show that an integer can always be found which contains only the digits 0 and 1 (in the decimal representation) and which is divisible by n.

   Solution: Look at the set of $n + 1$ numbers $\{1, 10, 10^2, \ldots, 10^{n-1}, 10^n\}$. There exists a subset of this set, whose sum is divisible by n. This was also an easy exercise in one of our previous homeworks for Pigeonhole Principle. But the sum of any subset of this set is an integer whose decimal representations has only 0s and 1s.

6. A certain locker room contains n lockers numbered $1, 2, 3, \ldots, n$ and all are originally locked. An attendant performs a sequence of operations $T_1, T_2, \ldots, T_n$, whereby with the operation T_k, $1 \leq k \leq n$, the condition of being locked or unlocked is changed for all those lockers and only those lockers whose numbers are multiple of k. He finishes these n operations and some doors will remain locked and some unlocked at the end. Do this for a few examples and guess which ones will remain locked and which ones remain unlocked. Prove your guess mathematically.

   Solution: We can see that for each number $1 \leq i \leq n$, we apply the operation on the ith locker for each of its divisors. Therefore the number of times that we do this operation is the same as the number of divisors of i. Therefore at the end the unlocked lockers are those whose number has an odd number of divisors. If $i = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the decomposition of i into primes then, as in problem set VII, one can see that the number of divisors of i is $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$. This number is odd if and only if all the numbers $a_1, a_2, \ldots, a_k$ are even. But then it easily implies that i is a perfect square. So, the locker will be unlocked if and only if its number is a perfect square.