SOLUTIONS TO HOMEWORK 3

MATH 437/537: PROF. DRAGOS GHIOCA

Problem 1. (6 points.) Let \( n \in \mathbb{N} \) and let \( a_1, \ldots, a_n, b \in \mathbb{Z} \). Prove that there exist integers \( c_1, \ldots, c_n \) such that
\[
a_1c_1 + \cdots + a_nc_n = b
\]
if and only if for each \( m \in \mathbb{N} \), the equation
\[
a_1x_1 + \cdots + a_nx_n \equiv b \pmod{m}
\]
is solvable.

Solution. One implication is clear. So, we are left to prove that if all of the above congruence equations are solvable, then the actual linear equation is solvable in integers. First, we note that if each \( a_i \) equals 0, then the conclusion is clear since \( b \equiv 0 \pmod{m} \) for all \( m \in \mathbb{N} \) if and only if \( b = 0 \). So, from now on, we assume not all of the \( a_i \)'s equal 0.

Next we let \( d \) be the greatest common divisor of all the numbers \( a_i \). Arguing identically as in the case of two integers, we obtain that \( d \) is the least positive integer expressible as a linear combination of the numbers \( a_i \). Furthermore, it’s clear that any integer is expressible as a linear combination (with integer coefficients) of the given \( a_i \)'s only if it’s a multiple of \( d \). So, in conclusion the linear equation
\[
a_1x_1 + \cdots + a_nx_n = b
\]
is solvable in integers if and only if \( d \mid b \). Now, if the linear congruence equation
\[
a_1x_1 + \cdots + a_nx_n \equiv b \pmod{d}
\]
is solvable, then clearly, \( d \mid b \). So, we obtained the desired conclusion.

Problem 2. (3 points.) Let \( d(n) \) be the number of positive divisors for the positive integer \( n \). Compute
\[
\lim \inf_{n \to \infty} \frac{d(n)}{\log(n)} \quad \text{and} \quad \lim \sup_{n \to \infty} \frac{d(n)}{\log(n)}.
\]

Solution. \( \lim \inf_{n \to \infty} \frac{d(n)}{\log(n)} = 0 \) since for each prime number \( p \) (and there exist infinitely many such numbers), we have that \( d(p) = 2 \) (while \( \log(p) \to \infty \)). On the other hand, we claim that
\[
\lim \sup_{n \to \infty} \frac{d(n)}{\log(n)} = \infty.
\]
Indeed, we consider all the numbers \( n \) of the form \( 6^k \); then \( d(n) = (k+1)^2 \) and so,
\[
\frac{d(6^k)}{\log(6^k)} = \frac{(k+1)^2}{k \log(6)} \to \infty \quad \text{as} \quad k \to \infty.
\]

Problem 3. (3 points.) Let \( n \) be a positive integer such that \( 2\phi(n) = n - 1 \) (where \( \phi(n) \) is the Euler-totient function). Prove that \( 3 \nmid n \).
Solution. Assume that for a positive integer $n$ satisfying $2\phi(n) = n - 1$, we have that $3 \mid n$. Then clearly, $3^2 \nmid n$ because then we would have that $3 \mid \phi(n)$ which contradicts the fact that $2\phi(n) = n - 1$ since $3 \nmid n - 1$. Moreover, $n$ itself must be a product of distinct primes since otherwise - if $p^2 \mid n$, say, then $p \mid \phi(n)$ but $p \nmid n - 1$ - contradiction. So, $n = \prod_{i=1}^{r} p_i$ for some primes

$$3 = p_1 < p_2 < \cdots < p_r.$$  

(Note that $2 \nmid n$ since otherwise $n - 1$ were odd, contradicting the fact that $2\phi(n) = n - 1$.) Now, if one of the primes $p_i$ (for $i = 2, \ldots, r$) satisfies $p_i \equiv 1 \pmod{3}$, then $3 \mid \phi(n)$, contradicting the fact that $3 \nmid n - 1$ (because $3 \nmid n$). So, we know that $p_i \equiv 2 \pmod{3}$ for each $i = 2, \ldots, r$.

But then

$$2\phi(n) = 4(p_2 - 1) \cdots (p_r - 1) \equiv 4 \cdot 1^r \equiv 1 \pmod{3},$$

which contradicts the fact that $n - 1 \equiv 2 \pmod{3}$ (because $3 \mid n$). This contradiction shows that indeed $3 \nmid n$.

Problem 4. (5 points.) Let $p_1 < p_2 < \cdots$ be the sequence of all prime numbers. Prove that for each positive integer $n$, there exists a positive integer $k$ such that the number $N := \prod_{i=n}^{n+k} p_i$ has the property that $\sigma(N) > 2N$, where $\sigma(N)$ represents the sum of all positive divisors of $N$.

Solution. We get that $\sigma(N) > 2N$ (for $N = \prod_{i=n}^{n+k} p_i$) if

$$\prod_{i=n}^{n+k} \left(1 + \frac{1}{p_i}\right) > 2.$$  

Now, for any positive real numbers $x$, we claim that

$$\log(1 + x) > x - x^2.$$  

Indeed, the function $f(x) := \log(1 + x) - x + x^2$ equals 0 for $x = 0$ and

$$f'(x) = -1 + 2x + \frac{2x^2 + x}{1 + x} > 0.$$  

So, $\prod_{i=n}^{n+k} \left(1 + \frac{1}{p_i}\right) > 2$ (for sufficiently large $k$) if the series

$$\sum_{i=1}^{\infty} \frac{1}{p_i}$$

diverges since we already know that the series $\sum_{i=1}^{\infty} \frac{1}{p_i}$ converges because even the entire series $\sum_{j=1}^{\infty} \frac{1}{j^2}$ converges. Now, in order to prove that the sum of the reciprocal of the prime numbers diverges to infinity, we employ two facts.

**Fact 1.** $- \log(1 - x) \leq 2x$ for all $0 \leq x \leq \frac{1}{2}$.

Indeed, the function $g(x) := 2x + \log(1 - x)$ equals 0 for $x = 0$ and

$$g'(x) = 2 - \frac{1}{1 - x} \geq 0$$

since $x \leq \frac{1}{2}$.

**Fact 2.** $\sum_{p} - \log \left(1 - \frac{1}{p}\right)$ diverges (where this sum is over all the primes $p$).
SOLUTIONS TO HOMEWORK 3

We have that for each \( n \in \mathbb{N} \), all the positive integers \( i \leq n \) may only be divisible by the first \( n \) prime numbers \( p_j \) (actually, in general, they are divisible by much fewer than those primes numbers) and so,

\[
\sum_{i=1}^{n} \frac{1}{i} < \sum_{e_1, \ldots, e_n \geq 0} \prod_{j=1}^{n} \frac{1}{p_j^{e_j}} = \prod_{j=1}^{n} \left( \sum_{e_j=0}^{\infty} \frac{1}{p_j^{e_j}} \right) = \prod_{j=1}^{n} \left( \frac{1}{1 - \frac{1}{p_j}} \right).
\]

Therefore, since the harmonic series diverges, we also get that the series \( \sum_p - \log \left( 1 - \frac{1}{p} \right) \) diverges.

Clearly, the combination of Facts 1 and 2 yields that \( \sum_p \frac{1}{p} \) diverges, which in turn finishes our proof.

**Problem 5.** (4 points.) Determine all positive integers \( n \) with the property that for each integer \( x \) coprime with \( n \) we have that \( x^2 \equiv 1 \pmod{n} \).

**Solution.** Let \( p^\alpha \) be a prime power dividing \( n \). The condition from the problem translates (due to Chinese Remainder Theorem) to asking that for each integer \( x \) coprime with \( p \), we have that \( x^2 \equiv 1 \pmod{p^\alpha} \). Now, if \( p \) were odd, then this yields that either \( p^\alpha \) divides \( x - 1 \) or it divides \( x + 1 \) since it cannot be that the prime \( p \) divides both \( x - 1 \) and \( x + 1 \). So, if \( p \) is an odd prime number, we would have that only 1 and \( p^\alpha - 1 \) are the only residue classes modulo \( p^\alpha \) which are coprime with \( p \); this can only happen if \( p = 3 \) and \( \alpha = 1 \).

Now, if \( p = 2 \), then we get that 2\(^\alpha \) must divide \( x^2 - 1 \) if \( x \) is an odd integer. Since 8 is the maximal power of 2 dividing \( x^2 - 1 \) when \( x \) is an arbitrary odd integer, we conclude that \( \alpha \in \{1, 2, 3\} \). So, in conclusion, \( n = 2^\alpha \cdot 3^\beta \) where \( 0 \leq \alpha \leq 3 \) and \( 0 \leq \beta \leq 1 \).

**Problem 6.** (3 points.) Show that there are arbitrary long sequences of consecutive positive integers, none of the numbers being of the form \( x^k \) for some \( k > 1 \).

**Solution.** Let \( N \) be a positive integer and let \( p_1, \ldots, p_N \) be distinct prime numbers. Then consider the system of congruences:

\[
x \equiv -i + p_i \pmod{p_i^2} \text{ for all } i = 1, \ldots, N.
\]

By the Chinese Remainder Theorem, this system is solvable and we consider a solution \( x_0 > 0 \). Then the positive integers \( x_0 + i \) (for \( i = 1, \ldots, N \)) are consecutive, each one of them is divisible by a prime number \( p_i \) but not divisible by a higher power of that prime number, which prevents each one of the numbers \( x_0 + i \) be of the form \( a^k \) for some integer \( k \geq 2 \).
Problem 7. (5 points.) Let $n$ be a positive integer. Find the number of solutions to the congruence equation

$$x^3 \equiv x \pmod{n}.$$  

Solution. Let $p^n$ be a prime power dividing $n$; so, if $x^3 \equiv x \pmod{p^n}$, which means $p^n \mid x(x-1)(x+1)$.

Now, if $p$ is odd, then out of $x, x-1$ and $x+1$, exactly one of them may be divisible by the prime $p$, which means that $p^n \mid x(x-1)(x+1)$ translates into one of the three possibilities $x \equiv -1, 0, 1 \pmod{p^n}$.

Now, assume $p = 2$. First of all, if $a = 1$ then any $x$ would work, i.e., there are two congruence classes modulo 2 = $p^n$. So, from now on, we assume $a \geq 2$. Then we have two possibilities: either $x$ is even, in which case $2^a \mid x(x-1)(x+1)$ implies $x \equiv 0 \pmod{2^a}$ (i.e., 1 solution), or $x$ is odd, in which case $x \equiv \pm 1 \pmod{2^a}$. If $x \equiv -1 \pmod{4}$, then $x-1 \equiv 2 \pmod{4}$ and then we must have $2^{a-1} | x+1$, which means that $x \equiv j \cdot 2^{a-1} - 1 \pmod{2^a}$ for $j \in \{0, 1\}$ if $a \geq 3$, while $x \equiv 3 \pmod{4}$ if $a = 2$. A similar answer we obtain if we analyze the other possibility: $x \equiv 1 \pmod{4}$. So, we obtain $1 + 2 \min(a-1, 2)$ solutions to the congruence equation $x^3 \equiv x \pmod{2^a}$.

Therefore, letting $n := \prod_{i=1}^N p_i^{n_i}$ (the prime power decomposition of $n$), the number of solutions to the congruence equation $x^3 \equiv x \pmod{n}$ is $\prod_{i=1}^N N_i$ (due to the Chinese Remainder Theorem), where each $N_i$ is either equal to 3 if $p_i$ is odd, or it equals to $1 + 2 \min(a_i-1, 2)$ if $p_i = 2$.

Problem 8. (6 points.) Let $\{a_n\}$ be the sequence given by $a_1 = 1$ and for $n > 1$, we have $a_n = n^{a_{n-1}}$.

What are the last two digits of $a_9$?

Solution. In order to determine the last two digits of $a_9$ it is sufficient to determine the residue class of $a_9$ modulo both 4 and 25. Now, since $a_9 = 9^{a_8}$ and $9 \equiv 1 \pmod{4}$, we conclude that also $a_9 \equiv 1 \pmod{4}$.

Now, in order to determine $a_9$ modulo 25, since $a_9 = 9^{a_8} = 3^{2a_8}$, it suffices to determine $a_8$ modulo $\phi(25)/2 = 10$ since we know that $3^{\phi(25)} \equiv 1 \pmod{25}$ by Euler’s Theorem.

In order to determine $a_8$ modulo 10, it suffices to determine $a_8$ modulo 2 and modulo 5. Since $a_8 = 8^{a_7}$, then clearly $a_8 \equiv 0 \pmod{2}$. On the other hand, in order to determine $a_8$ modulo 5, it suffices to determine $a_7$ modulo $\phi(5) = 4$ since $8^{\phi(5)} \equiv 1 \pmod{5}$ by Fermat’s Little Theorem.

We know that $a_7 = 7^{a_6}$ and since $7 \equiv -1 \pmod{4}$, while $a_6 = 6^{a_5}$ is even, we conclude that $a_7 \equiv 1 \pmod{4}$. So,

$$a_6 \equiv 8^1 \equiv 3 \pmod{5}.$$  

Therefore, $a_6 \equiv 3 \pmod{5}$ and $a_8 \equiv 0 \pmod{2}$, which yields $a_8 \equiv 8 \pmod{10}$. But then $2a_8 \equiv 16 \pmod{20}$.

So,

$$a_9 \equiv 3^{2a_8} \equiv 3^{16} \pmod{25}$$  

and then

$$3^{16} \equiv 9^8 \equiv 6^4 \equiv 11^2 \equiv 21 \pmod{25}.$$  

So, $a_9 \equiv 21 \pmod{25}$ and $a_9 \equiv 1 \pmod{4}$, which means that $a_9 \equiv 21 \pmod{100}$ and thus, the last two digits of $a_9$ are 21.