Amin Zolfagharian - 610300118

Problem 1.

suppose $x > 11$.

(a) if $x = 3k$ then we can write $x = 6 + (3k - 6)$. $(3k - 6 = x - 6 > 5)$.

(b) if $x = 3k + 1$ we can write $x = 4 + (3k - 3)$. $(3k - 3 = x - 4 > 7)$.

(c) if $x = 3k + 2$ we can write $x = 8 + (3k - 6)$. $(3k - 6 = x - 8 > 3)$.

since 4, 6 and 8 are all composite and $3k - 6$, $3k - 3$ are divisible by 3 and not 3 itself, they are all composite as well.

Problem 2.

We have:

$$100313 = 34709\ .\ 2 + 30895 \tag{1}$$
$$34709 = 30895\ .\ 1 + 3814 \tag{2}$$
$$30895 = 3814\ .\ 8 + 383 \tag{3}$$
$$3814 = 383\ .\ 9 + 367 \tag{4}$$
$$383 = 367\ .\ 1 + 16 \tag{5}$$
$$367 = 16\ .\ 22 + 15 \tag{6}$$
$$16 = 15\ .\ 1 + 1 \tag{7}$$

which shows that $\gcd(100313, 34709) = 1$. as for the linear combination we put $a = 100313$ and $b = 34709$.

$$(1) \implies 30895 = a - 2b$$
$$(2) \implies b = (a - 2b) + 3814 \implies 3814 = 3b - a$$
$$(3) \implies a - 2b = (3b - a).8 + 383 \implies 383 = 9a - 26b$$
$$(4) \implies 3b - a = (9a - 26b).9 + 367 \implies 367 = 237b - 82a$$
$$(5) \implies 9a - 26b = (237b - 82a).1 + 16 \implies 16 = 91a - 263b$$
$$(6) \implies 237b - 82a = (91a - 263b).22 + 15 \implies 15 = 6023b - 2084a$$
$$(7) \implies 91a - 263b = (6023b - 2084a) + 1 \implies 1 = 2175a - 6286b$$

Therefore we have:

$$2175 \times 100313 + 6286 \times 34709 = 1$$

Problem 3.

(i) Suppose $\gcd(a+b, \frac{a^p+b^p}{a+b}) = d$ and prime q such that $q \mid d$. if $q \mid a$ then $q \mid b$ which can not happen since $(a,b)=1$. Therefore $q \nmid a, b$ or $(q,a)=(q,b)=1$.

$$q \mid a+b \implies b \overset{q}{\equiv} -a \neq 0$$
$$q \mid a^{p-1} - a^{p-2}b + \cdots + b^{p-1} \overset{q}{\equiv} a^{p-1} - a^{p-2}(-a) + \cdots + (-a)^{p-1} = pa^{p-1}$$
$$(q,a)=1 \implies q \mid p$$

Therefore $q=p$ or $q=1$. If $p \mid a+b$ then $\gcd(a+b, \frac{a^p+b^p}{a+b}) = p$, otherwise it is 1.

(ii) Suppose $\gcd(n!+1, (n+1)!+1) = d$.

$$d \mid n!+1 \implies d \mid (n+1)! + n + 1 \tag{8}$$
$$d \mid (n+1)! + 1 \tag{9}$$
$$\implies d \mid n \implies d \mid n! \tag{10}$$
$$(8),(10) \implies d \mid n!+1-n! \implies d \mid 1 \tag{11}$$

Thus $\gcd(n!+1, (n+1)!+1) = 1$

Problem 4.

Lemma1. $x^a \overset{p}{\equiv} (x+kp)^a$.
Proof.

$$(x+kp)^a = x^a + \binom{a}{1}x^{a-1}kp + \cdots + (kp)^a$$
$$= x^a + p(\binom{a}{1}x^{a-1}k + \cdots + (kp)^{a-1}k) \overset{p}{\equiv} x^a$$

Suppose $f(x_0) = p$ for some prime p. Now for any $k \in \mathbb{Z}$ we have:

$$f(x_0+kp) \overset{p}{\equiv} a_n(x_0+kp)^n + a_{n-1}(x_0+kp)^{n-1} + \cdots + a_1(x_0+kp) + a_0$$
$$\text{Lemma1} \implies \overset{p}{\equiv} a_n x_0^n + a_{n-1}x_0^{n-1} + \cdots + a_1 x_0 + a_0 = f(x_0) = p$$

This shows that $p \mid f(x_0+kp)$ for any $k \in \mathbb{Z}$. Now assume there is no m such that $f(m)$ is composite. This means that all of $f(x_0+kp)$ are prime. And since $p \mid f(x_0+kp)$ therefore $f(x_0+kp) = p$ for all $k \in \mathbb{Z}$. but now consider the polynomial $g(x) = f(x) - p$. for all $k \in \mathbb{Z}$, $x_0 + kp$ is a root of $g(x)$. But this polynomial cannot have more than n roots since it is of degree n. Unless $g(x) \equiv 0$. Which means $f(x) \equiv p$. but since $n \geq 1$ it is not possible. The contradition shows that there must exists m, such that $f(m)$ is composite.

Problem 5.

(i)

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1) = p$$

Since $a, k > 1$ this means that $a^{k-1} + \cdots + a + 1 > 1$. Thus we must have $a - 1 = 1$ which implies $a = 2$. Now suppose k is composite. therefore we can write $k = mn$ such that $m, n > 1$.

$$a^{mn} - 1 = (a^m - 1)(a^{k-m} + a^{k-2m} + \cdots + a^m + 1)$$

Since both parentheses are greater than 1 then $a^k - 1$ cannot be prime. Therefore in order for $a^k - 1$ to be prime, k must be prime.

(ii) a must be odd otherwise $a^k + 1$ is even which means $2 \mid a^k + 1 = p$. which implies $p = 2$. but since $a, k > 1$ which means $a^k + 1 = 2$ is not possible. Now let p be an odd prime factor in k. $k = ps$. Let $b = a^s$.

$$a^k + 1 = b^p + 1 = (b+1)(b^{p-1} - b^{p-2} + \cdots - b + 1)$$

Since both parentheses are greater than 1 then $a^k + 1$ cannot be prime. This shows that for $a^k + 1$ to be prime k shouldn't have any odd prime factor, which means that it must be a power of 2.

Problem 6.

(i) $(\Rightarrow)$ Suppose $n \mid m$. There exists a k such that $m = kn$.

$$\begin{aligned} a^m - 1 &= (a^n - 1)(a^{m-n} + a^{m-2n} + \cdots + a^n + 1) \\ &\implies a^n - 1 \mid a^m - 1 \end{aligned}$$

$(\Leftarrow)$ Suppose $a^n - 1 \mid a^m - 1$. And suppose $m = nk + r$ where $0 \leq r < n$.

$$a^n - 1 \mid a^n - 1 \tag{12}$$

$$\implies a^n - 1 \mid (a^n - 1)a^{n(k-1)+r} = a^m - a^{n(k-1)+r} \tag{13}$$

$$(*) \implies a^n - 1 \mid a^{n(k-1)+r} - 1 \tag{14}$$

$$a^n - 1 \mid (a^n - 1)a^{n(k-2)+r} = a^{n(k-1)+r} - a^{n(k-2)+r} \tag{15}$$

$$(14), (15) \implies a^n - 1 \mid a^{n(k-2)+r} - 1 \tag{16}$$

$$\vdots$$

$$a^n - 1 \mid a^r - 1 \implies |a^n - 1| \leq |a^r - 1| \tag{17}$$

$$\implies a^n - 1 \leq a^r - 1 \tag{18}$$

which is impossible since $r < n$ unless $a^r - 1 = 0$ which means that $r = 0$. this shows that $m = nk$ and $n \mid m$.

(ii) Suppose $\gcd(a^n - 1, a^m - 1) = d$. without loss of generality suppose $m \geq n$. and let the euclidean algorithm for m and n be:

$$r_0 = m, \ r_1 = n$$
$$r_j = r_{j+1}q_{j+1} + r_{j+2}$$

for $j = 0, 1, \ldots, k-2$. and $r_k = 0$ and $r_{k-1} = \gcd(n, m)$. Now we use induction and show that if $d \mid a^{r_i} - 1$ and $d \mid a^{r_{i+1}} - 1$ then $d \mid a^{r_{i+2}} - 1$.

$$d \mid a^{r_i} - 1 \tag{19}$$
$$d \mid a^{r_{i+1}} - 1 \overset{\boldsymbol{(i)}}{\Longrightarrow} a^{r_{i+1}} - 1 \mid a^{r_{i+1}q_{i+1}} - 1 \tag{20}$$
$$\Longrightarrow d \mid (a^{r_{i+1}q_{i+1}} - 1)a^{r_{i+2}} = a^{r_i} - a^{r_{i+2}} \tag{21}$$
$$(19), (21) \implies d \mid a^{r_{i+2}} - 1 \tag{22}$$

This shows that $d \mid a^{r_{k-1}} - 1 = a^{\gcd(n,m)} - 1$. On the other hand by part ***(i)*** we know that $a^{\gcd(m,n)} - 1 \mid a^n - 1, a^m - 1$. Therefore $a^{\gcd(n,m)} - 1 \mid d$. Thus $d = a^{\gcd(m,n)} - 1$.

(iii) Let $\gcd(2^m - 1, 2^n + 1) = d$. $d \mid 2^n + 1 (*)$.

$$d \mid (2^n + 1)(2^n - 1) = 2^{2n} - 1$$
$$\boldsymbol{(ii)} \implies d \mid \gcd(2^m - 1, 2^{2n} - 1) = 2^{\gcd(m,2n)} - 1$$
$$\overset{m\ odd}{=} 2^{\gcd(m,n)} - 1 = \gcd(2^m - 1, 2^n - 1)$$
$$\implies d \mid \gcd(2^m - 1, 2^n - 1) \implies d \mid 2^n - 1$$
$$(*) \implies d \mid 2^n + 1 - (2^n - 1) = 2$$

But d cannot be 2 since $2^m - 1$ is odd. Therefore $d = 1$.

Problem 7.

Suppose prime number in form of $3k + 2$ are finite. and are all $p_1, p_2, \ldots, p_k$. Let $A = p_1^2 p_2^2 \ldots p_k^2 + 1$. Since this number if of form $3k + 2$ and is greater than all of p_is then it must be composite. Suppose prime p such that $p \mid A$. then $p \neq 3$ otherwise:

$$3 \mid 3r + 2 \implies 3 \mid 2$$

Which is a contradiction. Also if $p = 3r + 2$ then $p = p_i$ for some $1 \leq i \leq k$ then:

$$p_i \mid p_1^2 p_2^2 \ldots p_k^2 + 1 \implies p_i \mid 1$$

Which is a contradiction. then all of prime factors of A are of the form $3k + 1$. but this also cannot happen since product of $3k + 1$ numbers is also a $3k + 1$ number. But A is of form $3k + 2$. This contradiction shows that the number of primes in form of $3k + 2$ cannot be finite.

Problem 8.

$m = n$ for any $n \in \mathbb{Z}$ is an answer. Wihtout loss of generality $|m| > |n| > 1$. Let $d = \gcd(m, n)$. and $m = dm_1$ and $n = dn_1$ such that $\gcd(n_1, m_1) = 1$.

$$\begin{gathered}
n^m = d^m n_1^m \ , \ m^n = d^n m_1^n \\
\implies d^m n_1^m = d^n m_1^n \\
\implies d^{m-n} n_1^m = m_1^n \implies n_1^m \mid m_1^n \\
(n_1, m_1) = 1 \implies n_1^m \mid 1 \implies n_1 = \pm 1 \\
n = d \implies n \mid m = nk \\
n^{nk} = (nk)^n \implies (n^{k-1})^n = k^n \implies n^{k-1} = k \\
2^{k-1} \leq n^{k-1} = k
\end{gathered}$$

But this inequality holds for $k < 3$. If $k = 1$ then $m = n$. Which is an answer. If $k = 2$ then $m = 2n$.

$$n^{2n} = (2n)^n \implies n^n = 2^n \implies n = \pm 2$$

Therefore if $n = 2$ then $(m, n) = (4, 2)$ an answer for the equation. and if $n = -2$ then $(m, n) = (-4, -2)$ is also an asnwer.

Problem 9.

(i) Let $\gcd(n! \times i + 1, n! \times j + 1) = d$.

$$\begin{gathered}
d \mid n! \times i + 1 \implies d \mid n! \times ij + j \\
d \mid n! \times j + 1 \implies d \mid n! \times ij + i \\
\implies d \mid i - j
\end{gathered}$$

Since $i, j < n$ then $i - j < n$ which means that $i - j \mid n!$.

$$\begin{gathered}
d \mid i - j \mid n! \\
d \mid n! \times i + 1 \\
\implies d \mid 1
\end{gathered}$$

Thus $\gcd(n! \times i + 1, n! \times j + 1) = 1$.

(ii) Suppose prime numbers are finite and $P = \{p_1, p_2, \ldots, p_k\}$ are all of them. let $N > p_k > k$. then numbers $N! + 1, N! \times 2 + 1, \ldots, N! \times N + 1$ are all composite. but they don't have any commond divisors.which means each of primes in P can only divide one of them. But since we have N numbers and k primes and $N > k$ this is not possible. Which is a contradiction. Then P is not a finite set.