# ASSIGNMENT 2

## Problems

1. If $0 < b < a$, show that the number of steps to find $(a, b)$ by the Euclidean algorithm is at most $2(\log_2 b + 1)$.
2. (a) Suppose $a, b, c > 0$ and $(a, b)|c$. Show that the number of positive integral solutions (i.e., both $x$ and $y$ are positive) to the Diophantine equation $ax + by = c$ is $\left[\frac{c(a,b)}{ab}\right] + 1$.
(b) Does the linear equation $1961x + 2257y = 37370$ have an integer solution? If it does, describe the set of all integer solutions and determine how many of the solutions have both the coordinates positive.
3. Show that the following equations have no solution in integers:
(i) $x^3 - x + 320 = 0$,
(ii) $x^3 + 7y + 4 = 0$,
(iii) $x^4 + 66 = 10y^2 + 55$,
(iv) $6x^3 - y^2 - 31^2 = 0$,
4. Consider the curve $\mathcal{C} : y^2 - x^3 - 24x = 0$. Determine three rational points on $\mathcal{C}$ by inspection. Obtain a new rational points on $\mathcal{C}$ using these points.
5. Consider the curve $\mathcal{C} : y + x^3 - 4x = 0$. Determine the equation of the tangent to this curve at the point $(2, 0)$. Find the $x$-corrdinate of the point at which this tangent line intersect the curve $\mathcal{C}$.
6. Suppose $\mathcal{C} : (x - x_0)^2 + (y - y_0)^2 - r^2 = 0$ is a circle on the plane so that the centre both $x_0$ and $y_0$ are irrational numbers. Nothing is given about $r$. Show that $\mathcal{C}$ can have at most two rational points.
7. Is there any prime $p$ such that $6x^3 - p^2 - y^2 = 0$ has an integer solution?
8. Describe the set of all integer solutions to $2x^2 + xy - y^2 = 0$
9. Find all integers $a, b, c$ such that $a \equiv b (\text{mod } c)$, $b \equiv c (\text{mod } a)$, $c \equiv a (\text{mod } b)$.
10. Show that for any prime $p > 2$,
(a) $\binom{p}{k} \equiv 0 (\text{mod } p)$ for $1 \leq k \leq p - 1$,
(b)$\binom{p-1}{k} \equiv (-1)^k (\text{mod } p)$ for $0 \leq k \leq p - 1$,
(c)$(p - 2)! \equiv 1 (\text{mod } p)$,
(d) $\binom{p^r}{k} \equiv 0 (\text{mod } p)$ for $r \geq 1$ and $1 \leq k \leq p^r - 1$.
11. Show that for positive integers $a$ and $n$ with $a \geq 2$, $\phi(a^p - 1) \equiv 0 (\text{mod } p)$.
12. Find the smallest positive integer $n$ such that $2^n - 1$ is divisible by 2025.
13. Show that for any integer $n$, $n^5/5 + n^3/3 + 7n/15$ is an integer.
14. Show that if $a, b, c$ satisfy the equation $a^2 + b^2 = c^2$ then $60 \mid abc$.
15. Show that if $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.
16. Show that for $a$ odd, $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ for $n \geq 3$.
17. Suppose $n$ is odd. Prove that it is not possible that $n \mid (3^n + 1)$.
18. Suppose $p \mid (a^{2^r} + 1)$ for some $a$. Show that $p \equiv 1 \pmod{2^{r+1}}$.
19. Show that the system of congruences $a_i x \equiv b_i \pmod{m_j}$, $\quad i = 1, 2, \cdots, k$

has a solution if and only if for every pair $(i, j)$, one has $d_i \mid b_i$, where $d_i := (a_i, m_i)$ and $(b_j a_i - b_i a_j)/d_i d_j \equiv 0 \mod\big((m_i/d_i, m_j/d_j)\big)$. Show that in the above situation the solution is unique modulo
$[m_1/d_1, m_2/d_2, \cdots, m_k/d_k]$.
20. For $i = 1, 2, \cdots, k$, let there be positive integers $m_i$, nonnegative integers $d_i$ and polynomials $f_i(x) \in \mathbb{Z}[x]$ such that the number of distinct solutions modulo $m_i$ to the congruence $f_i(x) \equiv 0 \pmod{m_i}$ is $d_i$. Assume, moreover, that $m_i$'s are pairwise coprime. Show that the system of simultaneous congruences $f_i(x) \equiv 0 \pmod{m_i},\ i = 1, 2, \cdots, k$ admits exactly $d_1 d_2 \cdots d_k$ distinct solutions modulo $m_1 m_2 \cdots m_k$.
21. Let $S$ be the sum of the integers from 1 to 999 which are prime to 999. Write the prime power factorization of $S$. Explain your method.
22. Let $p$ be an odd prime and let

$$e_k(X_1, X_2, \cdots, X_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} X_{i_1} X_{i_2} \cdots X_{i_k},$$

for $k = 1, 2, \cdots, n$ denote the elementary symmetric polynomials. Show that $e_k(1, 2, \cdots, p-1)$ is divisible by $p$ for $k = 1, 2, \cdots, p-2$.
23. Let $p$ be an odd prime and let

$$S_k(X_1, X_2, \cdots, X_n) = \sum_{1 \le i \le n} {X_i}^k$$

for $k = 1, 2, \cdots$. Show that $S_k(1, 2, \cdots, p-1) \equiv 0 \pmod{p}$ if $k$ is not a multiple of $p-1$ and $S_k(1, 2, \cdots, p-1) \equiv -1 \pmod{p}$ otherwise.
24. Show that

$$\prod_{\substack{1 \le a \le p^\alpha \\ (a,p)=1}} a \equiv -1 \pmod{p^\alpha}.$$

25. Show that for any integer $n > 1$, the odd prime divisors of $n^4 + 1$ are congruent to 1 modulo 8.
26. Let, for any integer $q > 1$,

$$c_q = \sum_{\substack{1 \le a \le q-1 \\ (a,q)=1}} e^{2\pi i \frac{a}{q}}.$$

Show that $c_{q_1 q_2} = c_{q_1} c_{q_2}$ for $(q_1, q_2) = 1$. Hint: Use the explicit description of the reduced (i.e., coprime) residue classes modulo $q_1 q_2$.
27. Show that $x^4 + y^4 = z^2$ has no non-trivial solution using Fermat's method of descent and the explicit description of the Pythagorean triplets.
28. Prove that $\nu_f(n)$ is a multiplicative function, where, for a polynomial $f \in \mathbb{Z}[x]$, $\nu_f(n)$ denotes the number of zeros of $f$ modulo $n$.
29. Show that in Fermat's two square theorem, the representation of a prime as a sum of two squares is unique up to ordering.
30. Formulate a theorem describing a necessary and sufficient condition for existence of solutions (over $\mathbb{Z}$) to a congruence of the form

$$aX + bY + cZ = e,$$

where $a, b, c, e$ are integers, and prove it.
Using the above find all integer solutions to $6X + 15Y + 35Z = 1$.