2010 BdMO Summer Math Camp Number Theory Exercises

1. **Divisibility**: For any integer n, prove that $(21n+4)/(14n+3)$ is irreducible (cannot be be broken up into smaller pieces).

   Hint: Recall Bezout Bhai: if $ax+by=1$, then $(x,y)=1$.

2. Let n be a positive integer. Prove that $\text{GCD}(n!+1,(n+1)!+1)=1$.

   Hint: Bezout: $(n+1)\cdot n! - 1\cdot((n+1)!+1)=n$. The the gcd divides n

3. Let $F_k = 2^{2^k}+1,\ \ k \geq 0$. Prove that if $m \neq n$, then $\text{GCD}(F_m, F_n)=1$.

   Hint: If $m<n$ then $2^m+1 \mid 2^n-1$ then translate this in terms of F_m and F_n.

4. Let $a>1,\ \ m,n>0$, prove that: $D=\text{GCD}(a^m-1,a^n-1)=a^{\text{GCD}(m,n)}-1$.

   Hint: (1) To show that $D=a^{\gcd(m,n)}-1$, show that $a^{\gcd(m,n)}-1 \mid D$ and $D \mid a^{\gcd(m,n)}-1$. (2) Let $d=\gcd(m,n)$ then let $\alpha m-\beta n=d$ and since $D \mid a^m-1$ it also divides $a^{\alpha m}-1$ and thus divides $a^{\alpha m}-a^{\beta n}$.

5. Let $m,n>0,\ \ mn \mid (m^2+n^2)$, show that $m=n$.

   Hint: Let $d=\gcd(m,n)$, then $m=m_1d$ and $n=dn_1$ and $(m_1,n_1)=1$ and $m_1n_1 \mid m_1^2+n_1^2$.

6. Suppose that the GCD of the positive integers $,a,b,c$ is 1, and $(ab)/(a-b)=c$. Prove that $a-b$ is a perfect square.

   Hint: Use the relation $1=(a,b,c)=((a,b),c)=(d,c)$ where $d=(a,b)$ and thus $ab=a_1b_1d^2$.

7. Let k be a positive odd integer. Prove that $1+2+\cdots+n$ divides $1^k+2^k+\cdots+n^k$

   Hint: We want $\frac{n(n+1)}{2} \mid 1^k+\cdots+n^k$ which is equivalent to $n(n+1) \mid 2(1^k+\cdots+n^k)$. Use the pairing trick $2(1^k+\cdots+n^k)=(1^k+n^k)+(2^k+(n-1)^k)+\cdots+(n^k+1^k)$.

8. **Unique Factorization:** Show that among the infinite sequence 10 001, 100 010 001,..., there is no prime number.

   Hint: Let the nth term be a_n. Then $a_{2k}=\frac{10^{8k}-1}{10^4-1}=\frac{10^{8k}-1}{10^8-1}\cdot\frac{10^8-1}{10^4-1}$ and do the same a_{2k+1}.

9. Suppose that positive a,b,c, and d satisfy $ab=cd$. Prove that $a+b+c+d$ is not prime.

   Hint: Let $a/c=d/b=m/n$ then $a=um, b=un, d=vm, b=vn$.

10. Prove that if positive integers a,b satisfy $2a^2+a=3b^2+b$ then $a-b$ and $2a+2b+1$ are perfect squares.

    Hint: Factoring $b^2=(a-b)(2a+2b+1)$, let $d=\gcd(a-b,2a+2b+1)$. If $p \mid d$ then $p \mid b$.

11. Let n,a and b be integers, and $a \neq b$. Prove that $n \mid \frac{a^n-b^n}{a-b}$ if $n \mid (a^n-b^n)$.

Hint: Let p^e be the largest power of the prime p dividing n. Suppose p divides $t = (a - b)$. Use the binomial theorem to expand $\frac{a^n - b^n}{t}$ in powers of t to show that there are enough powers of t so that p^e divides $\frac{a^n - b^n}{t}$.

12. Let m, n be non-zero integers. Prove using algebraic methods that $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ is an integer.

    Hint: Map this problem to $\sum_k (\left\lfloor \frac{2m}{p^k} \right\rfloor + \left\lfloor \frac{2n}{p^k} \right\rfloor) \geq \sum_k \left\lfloor \frac{m}{p^k} \right\rfloor + \left\lfloor \frac{n}{p^k} \right\rfloor + \left\lfloor \frac{m+n}{p^k} \right\rfloor$

13. **Indeterminate equations**: If a positive integer, after adding 100 becomes a perfect square, and after adding 168, becomes another perfect square, find this number.

14. Find all integer solutions of the following indeterminate equation: $x^4 + y^4 + z^4 = 2x^2y^2 + 2y^2z^2 + 2z^2x^2 + 24$.

    Hint: Factor $(x + y + z)(x + y - z)((y + z - x)(z + x - y) = 3 \cdot 2^3$. Check whether any two of factors on the left have the same parity by adding them together.

15. Prove that the product of two consecutive positive integers is neither a perfect square nor a perfect cube.

    Hint: Let $x(x + 1) = y^3$. Since $(x, x + 1) = 1$, x and $x + 1$ must be cubes.

16. Prove that the equation $y^2 + y = x + x^2 + x^3$ has no integer solutions for $x \neq 0$.

    Hint: Factor into $(y - x)(x + y + 1) = x^3$, show that the $\gcd(y - x, x + y + 1) = 1$. let $u^3 = y - x$ and $v^3 = x + y + 1$. Then use a "size" argument to show that $v^3 - u^3 = 2x + 1$ which gives $2uv + 1 = (v - u)(v^2 + uv + u^2)$ cannot hold since $v > u$.

17. Let k be a given positive integer, $k \geq 2$. Prove that (a) the product of 3 consecutive integers is not a k-th power of some integers; (b) the product of 4 consecutive integers is not a k-th power of some integers also.

    Hint: (a) $(x^2 - 1, x) = 1$ and $u^k = x^2 - 1, v^k = x$, then $1 = u^k - v^k = (u - v)(u^{k-1} + \cdots + v^{k-1})$, now use a size argument to show that this product cannot be 1. (b) again factor and use a size argument.

18. **Congruences**: Let a, b, c, d be positive integers. Prove that $a^{4b+d} - a^{4c+d}$ is divisible by 240.

19. Let a, b, c be integers such that $a + b + c = 0$. Set $d = a^{1999} + b^{1999} + c^{1999}$. Prove that $|d|$ is not prime.

20. Assume that the integers x, y, z satisfy $(x - y)(y - z)(z - x) = x + y + z$.

21. Let $n > 1$, prove that $a = 111 \cdots 1$ is not a perfect square. There are n ones in a.

22. Using the digits $1, 2, 3, 4, 5, 6, 7$ we can get 7-digit numbers and every digit is used only once in every such 7-digit number. Prove that none of these numbers are multiples of each other.

23. Assume that the sequence $\{x_n\}$ is 1,3,5,11,... and satisfies the recursion relation $x_{n+1} = x_n + 2x_{n-1}$ for $n \geq 2$. The sequence $\{y_n\}$ is 7, 17, 55, 161,... and satisfies the recursion relation: $y_{n+1} = 2y_n + 3y_{n-1}$ for $n \geq 2$. Prove that these 2 sequences have no common terms.

24. Let p be a positive integer. Determine the minimum positive value of $(2p)^{2m} - (2p-1)^n$, where m, n are any positive integers.

25. By connecting the vertices of a regular n-gon we get a closed n-line. Prove that if n is even then among the connecting lines, there are only two parallel lines among the connecting lines, and that if n is odd then there are more than 2 parallel lines among the connecting lines.

26. Let $n > 3$ be an odd number. Prove that after arbitrarily taking out one element out from the n-element set $S = \{0, 1, ..., n-1\}$, we can always separate the rest of the elements into 2 groups, every group consists of $(n-1)/2$ numbers, and the the sums of the numbers in two groups are equal modulo n.

27. **Fermat, Euler, and Chinese Remainder Theorems**: Prove Fermat's theorem, Euler's theorem and state the Chinese Remainder Theorem.

28. Let p be prime. Prove that in the sequence $\{2^n - n\}$, $n \geq 1$ there are infinitely many composite numbers.

29. Prove that in the sequence 1,31, 331, 3331,... there are infinitely many composite numbers.

30. Show that for any given positive number n, there are n consecutive positive integers such that every such positive integer has a square divisor greater than 1.

31. For any given positive integer n, there are n consecutive positive integers such that all such numbers are not power numbers (a power number has a prime factorization where the power of each prime is greater than 1).

32. For a given positive integer n, let $f(n)$ be the minimal positive integer such that $\sum_{k=1}^{f(n)} k$ is divisible by n. Prove that $f(n) = 2n-1$ if and only if n is a power of 2.

33. Let n and k be given integers such that $n > 0$ and $k(n-1)$ is even. Prove that there are x and y such that $\text{GCD}(x, n) = \text{GCD}(y, n) = 1$ and $x + y = k(\text{mod } n)$

34. **Order**: Let $\text{GCD}(a, n) = 1$, then show that there is an $1 \leq r \leq n-1$ such that $a^r \equiv 1(\text{mod } n)$. Show that (1) if there is an N such that $a^N = 1(\text{mod } n)$ then $r \mid N$; (2) r divides $\phi(n)$ and $r \mid (n-1)$ if n is prime.

35. Assume $n > 1$ and $n \mid (2^n + 1)$ show that $3 \mid n$.

36. For $n > 1$, show that n doesn't divide $2^n - 1$.

37. Use infinite descent and contradiction to find another proof of the previous problem.

38. Let $n > 1$, and n be odd. Show that for any integer m that n doesn't divide $m^{n-1} + 1$.

39. Let p be an odd prime. Prove that any positive divisor of $(p^{2p} + 1)/(p^2 + 1)$ is congruent to 1 modulo $4p$.