Number Theory–An Olympiad Approach[1]

Manjil P. Saikia

Abstract. We give a collection of all the important number theoretic results that are useful for students participating in the Mathematical Olympiads. The results are given without detailed proofs. A seperate problem sheet has been provided. The proofs of most of the results discussed can be found in the books mentioned in the **References** section. It is assumed that the students have some familiarity with certain algebraic manipulation techniques and other basic things.

1. Preliminaries

Well Ordering Principle (WOP): Every nonempty set S of nonnegative integers contains a least element; that is, there is some integer a such that $a \leq b$ for all b's belonging to S.

Theorem 1.1. ***(Archimedean Property)*** *If a and b are any positive integers, then there exists a positive integer n such that $na \geq b$.*

Theorem 1.2. ***(First Principle of Finite Induction)*** *Let S be a set of positive integers with the following properties:*

- *The integer 1 belongs to S.*
- *Whenever the integer k is in S, the next integer $k+1$ must also be in S.*

Then S is the set of all positive integers.

Theorem 1.3. ***(Binomial Theorem)****If a and b are integers and n is a natural number then the general binomial theorem gives the relationship:*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n.$$

2. Some Results and Definitions

Number Theory requires extensive preparation but the prerequisites are very few. Almost all are covered in a standard school syllabus and the remaining ones were covered in the earlier section. The strategies are accquired over time by massive amount of problem solving. This section contains almost all of the main results and definitions that a student preparing for Olympiads must know. Note that in this section all the variables stand for integers unless otherwise noted.

Property 2.1. *If $b = aq$ for some $q \in Z$, then a divides b, and we write $a \mid b$.*

Property 2.2. ***(Fundamental Properties of the Divisibility Relation)***

- $a \mid b, b \mid c \Rightarrow a \mid c$.

[1]A series of lectures delivered at Darrang College, Tezpur, India.

- $d \mid a, d \mid b \Rightarrow d \mid ax + by$.

Property 2.3. ***(Division Algorithm)*** *Every integer a is uniquely representable by the positive integer b in the form $a = bq + r, 0 \leq r < b$.*

Property 2.4. ***(Euclidean Algorithm)*** *In the above representation of integers gcd(a,b)=gcd(b,r).*

Theorem 2.5. ***(Bézout's Identity)*** *The gcd(a,b) can be represented by a linear combination of a and b with integral coefficients such that, there are $x, y \in Z$, so that $gcd(a, b) = ax + by$.*

Theorem 2.6. ***(Euclid's Lemma)*** *If p is a prime, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.*

Theorem 2.7. ***(Fundamental Theorem of Arithmetic)*** *Every positive integer can be uniquely represented as a product of primes.*

Theorem 2.8. ***(Euclid)*** *There are infinitely many primes.*

Property 2.9. *$n! + 2, n! + 3, n! + 4, \cdots, n! + n$ are $(n - 1)$ consecutive composite integers.*

Property 2.10. *The smallest prime factor of a nonprime n is $\leq \sqrt{n}$.*

Theorem 2.11. *All pairwise prime triples of integers satisfying $x^2 + y^2 = z^2$ are given by $x =\mid u^2 - v^2 \mid$, $y = 2uv$ and $z = u^2 + v^2$, $gcd(u, v) = 1$ and $u - v$ is not divisible by 2.*

Notation 2.12. ***(Congruences)*** *If $m \mid a - b$ then we write $a \equiv b \ (mod\ m)$.*

Congruences can be added, subtracted and multiplied in a usual manner but they cannot be divided always.

Theorem 2.13. ***(Fermat's Little Theorem)*** *Let a be a positive integer and p be a prime, then $a^p \equiv a \ (mod\ p)$.*

The converse is however not valid.

Theorem 2.14. ***(Wilson's Theorem)*** *If p is a prime, then $(p - 1) \equiv -1 \ (mod\ p)$.*

Definition 2.15. ***(Euler's totient function)*** *$\phi(m)$ denotes the number of numbers less than m which are prime to m.*

Property 2.16. *$gcd(a, m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \ (mod\ m)$.*

Theorem 2.17. ***(Euler)*** *If a and m be relatively prime positive integers then, $a^{\phi(m)} \equiv 1 \ (mod\ p)$.*

Property 2.18. ***(Sophie Germain Identity)*** *$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$.*

Definition 2.19. *We define $ord_p(n)$, by the nonnegative integer k such that $p^k \mid\mid n$. Then,*

$$n = \Pi_{p:prime} p^{ord_p(n)}$$

Theorem 2.20. *Let A and B be positive integers, then A is a multiple of B iff $ord_p(A) \geq ord_p(B)$ holds for all primes p.*

Notation 2.21. *$\lfloor x \rfloor$ is the greatest integer less than or equal to x. $\lfloor x \rfloor$ is read as* floor of x.

Theorem 2.22. ***(De Polignac)*** *$ord_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$.*

Property 2.23.
- $\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$.
- $\lfloor \frac{\lfloor x \rfloor}{n} \rfloor = \lfloor \frac{x}{n} \rfloor$.
- $\lfloor x + \frac{1}{2} \rfloor =$ *the integer nearest to* x.

Theorem 2.24. ***(Hermite)*** $\lfloor nx \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{n} \rfloor + \ldots + \lfloor x + \frac{n-1}{n} \rfloor$.

Notation 2.25. *$\tau(n)$ denotes the number of divisors of the nonnegative integer n.*

Notation 2.26. *$\sigma(n)$ denotes the sum of the divisors of the nonnegative integer n.*

Theorem 2.27. *If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is a prime decomposition of n, then,*

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$$

Theorem 2.28. *With the notation of the previous theorem we have, $(2a_1 + 1)(2a_2 + 1) \cdots (2a_k + 1)$ distinct pairs of ordered positive integers (a, b) with $lcm(a, b) = n$.*

Theorem 2.29. *For any positive integer n, $\Pi_{d|n} d = n^{\frac{\tau(n)}{2}}$.*

Theorem 2.30. *With the same notation as the above three theorems we have,*

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdots \frac{p^{a_k+1} - 1}{p_k - 1}.$$

3. Acknowledgements

The author wishes to thank Prof. M. B. Rege for [1] and R. C. Deka for inviting the author to deliver the lectures.

References

[1] T. Andreescu, D. Andrica and Z. Feng, *104 Number Theory Problems From the Training of the USA IMO Team*, Brikhäuser, 2007.
[2] D. M. Burton, *Elementary Number Theory*, Sixth Edition, McGraw Hill, 2010.
[3] A. Engel, *Problem–Solving Strategies*, Springer, 2005.
[4] H. Lee, T. Lovering and C. Pohoată, *INFINITY*, 2008.

Department of Mathematical Sciences, Tezpur University, Sonitpur, Pin-784028
E-mail address: manjil_msi09@agnee.tezu.ernet.in, manjil.saikia@gmail.com