Basic Number Theory

Masum Billal
University Of Dhaka
Department of Computer Science and Engineering
Dhaka
Bangladesh
Email: billalmasum93@gmail.com

November 23, 2015

Contents

The note has been separated into two parts, one discusses most of the basic ideas in divisibility and the other have only problems. The problems are not attached with the sections where the ideas have been discussed. It has been separated for the purpose that you don't know what you have to use while solving the problems. Solving problems while discussing particular theory, it becomes almost obvious which idea you should invoke. But in real, when the competition arises, we don't know which theorem is going to rescue us. To have a skill for identifying the perfect theorem needed to solve a problem, the problems have become another part of this note. Moreover, the problems are divided into two. Some problems are solved, and the others are left for practices.

Further Reading

The following books are strongly recommended for further reading. Probably it is the order they should be arranged. The books with lower numbering should be read first.

1. *Art And Craft Of Problem Solving*, by *Paul Zietz*.
2. *Problem Solving Strategies(Chapter 6-Number Theory)*, by *Arthur Engel*.
3. *104 Number Theory Problems*, by *Titu Andreescu, Dorin Andrica, Zuming Feng*.
4. *Number Theory, Structures, Examples And Problems*, by *Titu Andreescu, Dorin Andrica*.
5. *Number Theory*, by *S.G. Telang*.

Then you are able to read any book further. Note that the theorem book of Telang is put in the last position. You might think that this book should appear at first. In our country, it is considered the more theorems you know the more problems you can solve in number theory. In fact, this is false. *Everything is almost in vain without intuition.* So, before learning any theorem, you have to learn how to think and implement those properly. Without intuition, you may not be able to apply the theorems already learnt. When you read the first and second book, you have to use almost no theorem to solve problems. By this process you gain an ability to understand what the best theorem to be invoked here is. If you learn theorems after having a minimum intuition, then you can understand yourself what you have learnt. Then the last book can help you the most.

Part I

Foundations Of Divisibility And Congruence

Chapter 1

Divisibility

1.1 Definitions

Note the following division of 97 by 24.

$$97 = 24 \cdot 4 + 1$$

In this division, we call 4 the *quotient* and 1 the *remainder* of this division. For the division $96 = 24 \cdot 4 + 0$, we have the remainder 0. In this case, we say that 96 is divisible by 24 and 4 both.

Definition 1. Let a and b be two natural numbers such that b leaves a remainder 0 upon division by a. Then b is said to be *divisible* by a. We denote it by $a|b$. Sometimes, the notation $b \vdots a$ is also used but in this note, we shall make the most common use of the notation of $a|b$.

Here, a is called a *divisor* of b and b is a *multiple* of a. If b leaves a remainder other than 0, then b is not divisible by a and is denoted by $a \not| b$.

Example. $7|343$, 565655 is a multiple of 5, 29 is a divisor of 841 and so on.....

Try some more examples and make sure with the notations and definitions of divisibility. Because your further reading of this note requires this excellency.

Definition 2. If any positive integer is not divisible by any positive integer except 1 and that number, we call this special number a *prime*. Alternatively,

a number[1] is prime if and only if[2]

Prime number is the most useful in number theory, and it is the block builder of the entire number theory.

Example. 2 is the only even prime. If an even number is greater than 2, then it must be divisible by 2. Thus, it can't be a prime. First 3 odd primes are $3, 5, 7$.

Definition 3. If a number leaves remainder 0 upon division by 2, then it is called *even*. If it leaves the remainder 1, then it is called *odd*. The property of a number being even or odd is called *parity*. Two numbers are of the *same pairity* if they both are odd or both are even. Otherwise they are of opposite parity. In other words, if two numbers give same remainder upon division by 2, they are of the same parity, else opposite.

Example. 5 and 7 are of the same parity, whereas 4 and 3 are not.

Check the truth of the following claims:

1. The sum and difference of two numbers of the same parity is even.
2. The sum and difference of two numbers of different parity is odd.
3. Increasing or decreasing a number by a multiple of 2 does not change the parity.
4. Any odd multiple of a number has the same parity of the number, and for even multiple has a parity even.

---

[1] We may call 'positive integers' generally 'number', if not stated.

[2] A proposition is said to be a *'if and only if'* or *'iff'* one when both the claim and the converse is true. For example, consider the following claim:

Every number divisible by 6 is even.

But the converse is :

Every even number is divisible by 6

The first claim is true whereas the second one is not. So, it is not a *iff* statement. Check that the following claim:

Every even number is divisible by 2.

is an *if and only if one*.

For this, the notation $\iff$ is used. For the example above,

x is even $\iff$ x is divisible by 2.

5. The parity remains unchanged after raising to a power.

These claims often come to the role. Note also the converse of them are true as well.

1.2 Properties Of Divisibility

Now, we see some corollaries that follow from the divisibility issue of a and b. These proofs are very simple. We shall use them while solving problems later. It is notable as well that, all the parameters involving divisibility generally are positive integers. If not stated in the problem, we may assume so. Because it is totally nonsense about discussing the divisibility of numbers with fractional part.

1. If $a|b$, then $\frac{b}{a}$ must be a positive integer.

   Let
   $$\frac{b}{a} = k$$
   Then $b = ak$. Thus, if $a|b$, there exists a unique positive integer (in fact, it is the quotient of the division of a and b) such that $b = ak$. Also, note that the relation $k|b$ is true.

2. Obviously $a|a$ and $a|0$ for all $a \in \mathbb{Z}$.

3. If $a|b$, then $a|-b$ or $-a|b$ or $-a|-b$.

4. If $a|b$, of-course $b \geq a$. Since every factor of a must be included in the factorization of b, b must be greater than or equal to a. The only possible case when $b < a$ is $b = 0$.

   Specially, if $a, b \in \mathbb{N}$ and $a|b$, then $b \geq a$.

5. If $a|b$ and $b|a$, then it easily follows from #3 that $a = b$ must hold.

6. If $a|b$ and $b|c$, then $a|c$ too. Let $b = ak, c = bk'$. Then, $c = akk'$ which implies $a|c$.

7. If $a|b$, then $ac|bc$ too and the converse is also true that is, if $ac|bc$, then $a|b$. This is straight forward. If $ac|bc$, $\frac{bc}{ac} = \frac{b}{a}$ is a positive integer, or $a|b$.

8. If $a|b$ and $a|c$, then any combination of b and c is divisible by a. In other words,
$$a|bx + cy$$
for integers x, y.
Important cases are
$$a|b \pm aq$$
$$a|b \pm c$$
$$a|b \pm a$$

9. If $d|p$, then $d = 1$ or $d = p$.

10. If $a|b$, every prime divisor p of a also divides b.[3]

11. (*Euclid's Lemma*) If p is a prime such that $p|ab$, then $p|a$ or $p|b$.

12. If $a \not| b$, then it must leave a remainder other than 0. Say, it is r. Then, $b - r$ would be divisible by a. Let
$$b - r = aq \text{ or } b = aq + r$$
Now, we prove that this r is a unique positive integer if $0 < r < a$.
For the sake of contradiction, suppose that
$$b = aq_1 + r_1 = aq_2 + r_2$$
with $r_1, r_2 < a$. From the latter, we get
$$a(q_1 - q_2) = r_2 - r_1$$
This equation says that $a|r_2 - r_1$. But $r_2 - r_1 < a$, a contradiction !!

13. For all composite [4] $n > 1$, n has a prime divisor p such that
$$p \leq \sqrt{n}$$
Assume that the smallest prime factor of n is p. Then $n = pk$ for some $k \geq p$. If $k < p$, then k would have at least one prime factor less than p, but that is not possible. Therefore, $k \geq p$. Then
$$n = kp \geq p^2$$
$$\Rightarrow p \leq \sqrt{n}$$
Using this property, we can determine whether a number is a prime or not. Though this is not an efficient approach at all, it is very useful for small numbers.

[3] Specially it is useful to consider the smallest prime factor of a which divides b.

[4] the numbers which is the product of two numbers at least 2 is called a *composite number*

1.3 Some Basic Combinatorial Identities

Some most useful notions in combinatorics are:

- n factorial $n!$ is the product of the first n positive integers. It is defined as:
$$n! = \begin{cases} 1 & \text{if } n = 0 \text{ or } 1 \\ 1 \cdot 2 \cdots n & \text{otherwise} \end{cases}$$
In other words, we can say that n is the number of permutations of n distinct balls without any repetition. [5]

- The binomial coefficient for two positive integers n and k is denoted by $\binom{n}{k}$ or $n\mathbf{C}_k$ or $\mathbf{C}_{n,k}$ or $\mathbf{C}_n^k$where $n \geq k \geq 0$.[6] And it is read as n *choose* k.

  It can be formulated as,
$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$
  Practically, it means the number of ways to choose k distinct persons from a pool of n distinct persons.

- ${}^n\mathbf{P}_k$ is the number of permutations or arrangements (i.e. considering orders with the combination) to take k distinct balls at a time from n distinct balls without any repetition. It is formulated as
$${}^n\mathbf{P}_k = \frac{n!}{(n-k)!}$$
  Note that if we take n at a time, then
$${}^n\mathbf{P}_n = n!$$
  Remember the definition of $n!$.

Identity 1.
$$\binom{n}{k} = \binom{n}{n-k}$$

[5] can you make the sense $0! = 1$.

[6] Note that $n < k$ does not make any sense. We can never choose 4 apples from 3. So, the sense implies that for $n < k$,
$$\binom{n}{k} = 0$$

We can prove this using the formula of $n!$ and the definition of $\binom{n}{k}$. But here a combinatorial proof is preferred since it makes a better sense.[7]

Combinatorial Proof. Think cleverly. When we separate k arbitrary people from a pool of n persons, for every choice we make, there are $n-k$ left as not chosen. Therefore, the number of ways k people are chosen is equal to the number of k people are left behind the choice. The latter number is of-course $\binom{n}{k}$. Now it is obvious that

$$\binom{n}{k} = \binom{n}{n-k}$$

□

Identity 2.

$${}^{n}\mathbf{P}_{k} = k! \cdot \binom{n}{k}$$

Proof. Note that the number of permutations remains same if we first choose k persons and then permute them. We can choose k persons in $\binom{n}{k}$ ways. Then we can re-permute them in $k!$ ways. Now it is obvious that,

$${}^{n}\mathbf{P}_{k} = k! \cdot \binom{n}{k}$$

□

[7] Try the algebraic proof yourself.

Chapter 2

GCD And LCM

We shall now discuss what the greatest common divisor and least common multiple of two numbers is.

Definition 4. Both the numbers a and b has several divisors. It is a common incidence that they have some same divisors. But the greatest one among them is a *unique* number. This one is called the *greatest common divisor* or *highest common factor* of a and b. This is frequently denoted by $gcd(a, b)$ or $hcf(a, b)$.

Sometimes it is denoted shortly by (a, b) only. In this note, we shall use this notation for brevity. When $(a, b) = 1$ that is two numbers don't have a common divisor other than 1, then a is called to be *co-prime* or *relatively prime* with b and is denoted by $a \perp b$.

Example. $(6, 28) = 2$, because 2 is the most common part among them. $56 \perp 243$, since 56 and 243 don't share any common factor other than 1.

As a consequence of *gcd*, the idea of least common multiple comes.
There are obviously an infinite multiples of a and b, namely

$$a \cdot 1, a \cdot 2, \ldots\ldots$$

$$b \cdot 1, b \cdot 2, \ldots\ldots$$

But their is a *unique smallest* multiple which is a multiple of both a and b. This is called the *least common multiple* of a and b.

Definition 5. The smallest positive integer that is divisible by both a and b is called the least common multiple of a, b. The notation $lcm(a, b)$ or $[a, b]$ is used to denote the least common multiple. For brevity,we shall use the notation $[a, b]$.

Example. $[24, 40] = 120$.

Note. We can extend this for more numbers too. You can of-course find the *gcd* of more than two numbers. Similarly, you may find out the *lcm* of more than two numbers too.

2.1 Properties Of GCD And LCM

From the definition of *gcd* and *lcm*, we get the following facts involving divisibility.

1. $(a, b)|a$ and $(a, b)|b$.
2. $a|[a, b]$ and $b|[a, b]$.
3. $(a, b)|[a, b]$ and so $[a, b] \geq (a, b)$.
4. If $d|a$ and $d|b$, then $d|(a, b)$. Because (a, b) is the greatest among the factors of a and b.
5. Every prime divisor of a and b divides $[a, b]$.
6. Every prime divisor of $(a, b)|a, b$.
7. $(a, b)|ax + by$ for any integers x, y. This is actually a corollary of divisibility property #7.
8. If $a = (a, b) \cdot a', b = (a, b) \cdot b'$, then $a' \perp b'$. This is very easy to sense. Since, (a, b) is the greatest among the common divisors, if (a', b') shares a common divisor, say d, then this would contradict the maximality of (a, b). Otherwise, we could multiply d with (a, b) with d which would yield a *gcd* greater than (a, b) namely, $d \cdot (a, b)$. Thus, $d = 1$.
9. $(a, a) = a$ and $(ak, bk) = k(a, b)$.
10. $(a, 1) = 1$ and $(a, 0) = a$.
11. If $b = aq + r$, then $(a, b) = (a, r)$.

    From the divisibility facts we noted above, $(a, b)|a$ and

    $$(a, b)|b = aq + r$$

    So,

    $$(a, b)|aq + r - (a \cdot q) = r$$

Corollary 1. Two special cases are :

$$(a, a+1) = 1$$

$$(a, a+b) = (a, b)$$

12. $a \geq (a, b)$ and $b \geq (a, b)$.

13. $[a, b] \geq a$ and $[a, b] \geq b$.

    Note. Equality occurs in the previous two inequalities iff $a = b$.

14. For a prime p, either $(p, a) = 1$ or $(a, p) = p$.

    Since p is a prime, $p|a$ or $p \not| a$. So, $a \perp p$ when $p \not| a$ and $(a, p) = p$ when $p|a$.

15. If $a \perp c$, then $(a, bc) = (a, b)$. This is true because c won't share any common factor with a. So, the *gcd* would remain unchanged.

16. If $a|bc$ with $a \perp c$, $a|b$.

    Corollary 2. If $a|c, b|c$ then $[a, b]|c$. In general, if

    $$a_1, a_2, \ldots\ldots, a_n | N$$

    then,

    $$[a_1, a_2, \ldots\ldots, a_n] | N$$

    Corollary 3. If

    $$a_1, a_2, \ldots\ldots, a_n | N$$

    with $a_1, a_2, \ldots, a_n$ pairwise co-prime integers, then $a_1 a_2 \cdots a_n | N$.

17. If m is a positive integer divisible by both a and b, then $[a, b]|m$ and $m \geq [a, b]$.

18. A very important theorem:

    $$(a, b) \cdot [a, b] = a \cdot b$$

    Here, we shall prove this only using the definition of (a, b) and $[a, b]$ to make a better sense.

    According to the definition, (a, b) is the greatest common part of a and b. On the other hand, $[a, b]$ contains both the common and uncommon parts of a and b (recall #3). Thus, (a, b) is included in $[a, b]$. Let the

uncommon part that is left except (a, b) is u_a, and the uncommon part of b is u_b. Then

$$a = (a, b) \cdot u_a, b = (a, b) \cdot u_b$$

It follows that

$$[a, b] = (a, b) \cdot u_a \cdot u_b$$

Note that

$$(a, b) \cdot [a, b] = (a, b)^2 \cdot u_a \cdot u_b$$

Also,

$$ab = (a, b)^2 \cdot u_a \cdot u_b$$

Thus, it is proved.

19. If $a \perp b$, then

$$a^m \perp b^n$$

for positive integers m, n.

20. If $a|b, (a, b) = a$.

2.2 Useful Identities In Divisibility

In this section, we are going to discuss some extremely useful identities in number theory. We will recall them later.

Identity 3 (*Sophie Germain Identity*)**.**

$$a^4 + 4b^4 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2)$$

Proof. Note:

$$\begin{aligned} &a^4 + 4b^4 \\ &= (a^2)^2 + 2 \cdot a^2 \cdot 2b^2 + (2b^2)^2 - 4a^2b^2 \\ &= (a^2 + 2b^2)^2 - (2ab)^2 \\ &= (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2) \end{aligned}$$

□

Corollary 4. If both $a, b > 1$ then $a^4 + 4b^4$ is a product of at least two numbers greater than 1 i.e. $a^4 + 4b^4$ is composite. The only case when it is prime is $a = b = 1$. Then $a^4 + 4b^4 = 5$, a prime.

Identity 4. For any positive integer n

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

Proof. This can be proved in many ways. One way is to use geometric series. Denote the sum,

$$S = a^{n-1} + a^{n-2}b + \ldots\ldots + ab^{n-2} + b^{n-1}$$

Note that

$$S \cdot a = a^n + a^{n-1}b + \ldots\ldots + ab^{n-1} \qquad (\dagger)$$

And,

$$S \cdot b = a^{n-1}b + \ldots\ldots + b^n \qquad (\ddagger)$$

Subtract $(\ddagger)$ from $(\dagger)$. We get,

$$S(a-b) = a^n - b^n$$

Which gives us

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

This proves the fact.

□

Corollary 5.

$$a - b | a^n - b^n$$

for all $n \in \mathbb{N}$

Corollary 6. If n odd, then

$$a^n + b^n = a^n - (-b)^n$$

Thus,

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

This is very useful, specially,

$$a + b | a^n + b^n$$

for all odd n.

Identity 5 (*Fibbonacci-Brahmagupta Identity*)**.**

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2 = (ad+bc)^2 + (ac-bd)^2$$

More generally,

$$(a^2+nb^2)(c^2+nd^2) = (ac-nbd)^2 + n(ad+bc)^2 = (ac+nbd)^2 + n(ad-bc)^2$$

The proof is rather straight forward comparison of both sides. So, let's avoid them.

Corollary 7. The products of two numbers of the form a^2+b^2 is of the same form.

Identity 6 (*Bhaskara's Lemma*)**.**

$$y^2 - Nx^2 = k$$

$$\Rightarrow \frac{(mx+Ny)^2}{k} - N(\frac{mx+y}{k})^2 = \frac{m^2-N}{k}$$

Proof. This is only straight algebraic manipulation.

Multiply both sides of the equation by m^2-N, add $n^2x^2+2mNxy+Ny^2$ and divide by k^2. We shall get the desired result. Check this by hand !

□

Remark 1. This is highly used in solving *Pell-Fermat Equations.*

Identity 7 (*Bézout's Identity*)**.** There exist integers x, y (not necessarily positive) such that

$$ax + by = (a, b)$$

Note. Such x and y are not unique. (why?)

Hope, you can make the sense about the truth of this theorem. So, I am avoiding the proof. Because I don't like this proof much.

Hint. Use *gcd* property #7 and divisibility property #7.

Corollary 8. If $a \perp b$, then there exists integers x and y such that

$$ax + by = 1$$

Identity 8.

$$(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$$

Proof. We use Euclidean algorithm to prove this.

Without loss of generality, we may assume that, $m \geq n$. If $m = n$, obviously

$$(a^m - b^m, a^m - b^m) = a^{(m,m)} - b^{(m,m)} = a^m - b^m$$

So,we have to prove this for $m > n$. Assume $m = n + k$.

Note that,

$$a^m - b^m = a^{n+k} - b^{n+k} = a^k(a^n - b^n) + b^n(a^k - b^k)$$

This yields

$$(a^m - b^m, a^n - b^n) = (a^n - b^n, a^k - b^k)$$

This is the step of Euclidean algorithm. So, repeating this process, we shall eventually get that

$$(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$$

□

Chapter 3

Congruence

Congruence is another basic part of number theory. As we said before, we may call congruence the dual of divisibility. It was first introduced and highly used by *Carl Fredrich Gauss*.

3.1 Definitions

Definition 6. If two integers a and b leaves the same remainder upon division by n, then a and b are said to be *congruent* modulo n. In other words, a leaves remainder b upon division by n.

Example. Since 14 and 62 leaves the same remainder 6 upon division by 8, we say that 14 and 62 are congruent modulo 8.

We denote it by $14 \equiv 62 \pmod 8$ and say 14 congruent to 62 modulo 8. Likewise,

$$11 \equiv 4 \pmod 7$$

In general, $a \equiv b \pmod n$. Note that these remainders can be negative. So, we can also take

$$11 \equiv -1 \pmod 6$$

Definition 7. b is the *residue* of a. If $0 \leq b < n$, b is called the *minimal residue* of a. Moreover, when $|b| \leq \frac{n}{2}$, then b is called the *absolute minimal residue*.

Definition 8. The set

$$\mathbb{Z}[n] = \{0, 1, 2, \ldots\ldots, n-1\}$$

is called the *complete set of residue class modulo* n. But we generally take the set

$$\mathbb{Z}[n] = \{1, 2, \ldots\ldots n-1\}$$

so that 0 can't create any problem. This is called a complete set of residue class modulo n because any integer gives a remainder upon division by n which is an element of this set. Also, it is obvious that every integer gives a unique remainder upon division by n which belongs to this set. This actually follows from #10 of divisibility.

Definition 9. $P(x)$ is a *polynomial* a sum of some powers of x (obviously finite). That is

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x + a_0$$

Here, n is the highest power of this polynomial, which is called *degree*.

3.2 Propositions

Proposition 1.

$$a \equiv b \pmod{n} \Rightarrow n|a-b$$

Note. The converse also holds (why?) i.e.

$$n|a-b \Rightarrow a \equiv b \pmod{n}$$

Proposition 2. For all $a \in \mathbb{Z}$, $a \equiv a \pmod{n}$

This holds because

$$n|a-a=0$$

Proposition 3. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

Since

$$a \equiv b \pmod{n} \Rightarrow n|a-b$$

This also implies

$$n|b-a$$

So,

$$b \equiv a \pmod{n}$$

Proposition 4. If

$$a \equiv b \pmod{n}$$

$$a + nq \equiv b \pmod{n}$$

When $a + nq$ is divided by n, the remainder is a. So, this is true.

Corollary 9.

$$a \equiv b \pmod{n} \Rightarrow a \pm b \equiv b \pmod{n}$$

Proposition 5. If

$$a \equiv b \pmod{n}$$

and

$$b \equiv c \pmod{n}$$

then

$$a \equiv c \pmod{n}$$

From the first two congruences see that,

$$n|a - b$$

and

$$n|b - c$$

Then,

$$n|a - b + b - c = a - c$$

This gives,

$$a \equiv c \pmod{n}$$

Proposition 6. If

$$a \equiv b \pmod{n}$$

and

$$c \equiv d \pmod{n}$$

then,

$$a + c \equiv b + d \pmod{n}$$

If you divide 123 by 5, the remainder is 3 and if 3424 is divided, then 4 is the remainder. Now, it makes the sense that when $123 + 3424$ is divided by 5, the remainder would be $3 + 4 = 7$ or 2. The claim makes sense. It is easy to prove as well. The rest is only to note:

$$a \equiv b \pmod{n} \Rightarrow n|a - b$$

$$c \equiv d \pmod{n} \Rightarrow n|c - d$$

Therefore,

$$n|a - b + c - d = (a + b) - (c + d)$$

Thus,

$$a + b \equiv c + d \pmod{n}$$

Proposition 7. For any integer c, if

$$a \equiv b \pmod{n}$$

then

$$ac \equiv bc \pmod{n}$$

Note that if,

$$a \equiv b \pmod{n}$$
$$a \equiv b \pmod{n}$$

adding we get,

$$2a \equiv 2b \pmod{n}$$

Again, adding,

$$3a \equiv 3b \pmod{n}$$

Applying c times,

$$ac \equiv bc \pmod{n}$$

Corollary 10. For $1 \leq i \leq n$, if

$$a_i \equiv b_i \pmod{n}$$

then,

$$a_1 a_2 \cdot \cdots \cdot a_n \equiv b_1 b_2 \cdot \cdots \cdot \pmod{n}$$

Corollary 11.

$$a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$$

Apply proposition-6 for k times and multiply them, you shall get the result.

It seems that congruences work like equations. We can add, subtract, multiply just like what we do in the equations. Now, what about division in congruence¿ Is it possible that if

$$ac \equiv bc \pmod{n}$$

then,

$$a \equiv b \pmod{n}$$

The answer is yes, but with a condition! Let's see what happen during division.

Consider the following congruence.

$$75 \equiv 50 \pmod{5}$$

If we could divide in general, then the congruence should be

$$3 \equiv 2 \pmod 5$$

after division by 25. But this is wrong. So, where the problem is? We can write this as

$$5|75 - 50 = 25(3 - 2)$$

Here, the factor 25 contain 5 only. If we divide this by 25, we are already discarding this factor. So, it will definitely hamper our congruence. From #16 of *gcd*, of-course we need a factor c which is co-prime to n. Thus, we have the following proposition.

Proposition 8. If

$$ac \equiv bc \pmod n$$

then

$$a \equiv b \pmod{\frac{n}{(n,c)}}$$

Corollary 12. If $c \perp n$, and

$$ac \equiv bc \pmod n$$

then,

$$a \equiv b \pmod n$$

Remark 2. We shall call this *cancellation rule*.

Proposition 9. If

$$a \equiv b \pmod n$$

then

$$P(a) \equiv P(b) \pmod n$$

From the definition of polynomial,

$$P(a) = a_n a^n + a_{n-1}a^{n-1} + \ldots\ldots + a_1 a + a_0$$

Similarly,

$$P(b) = a_n b^n + a_{n-1}b^{n-1} + \ldots\ldots + a_1 b + a_0$$

We need to prove that $P(a)$ and $P(b)$ are congruent modulo n.
Note that,

$$a^n \equiv b^n \pmod n$$
$$\Rightarrow a_n a^n \equiv a_n b^n \pmod n$$

Likewise,

$$a_{n-1}a^{n-1} \equiv a_{n-1}b^{n-1} \pmod{n}$$
$$\cdots\cdots\cdots\cdots$$
$$a_1 a \equiv a_1 b \pmod{n}$$
$$a_0 \equiv b_0 \pmod{n}$$

Add them. We get

$$a_n a^n + a_{n-1}a^{n-1} + \ldots\ldots + a_1 a + a_0 \equiv a_n b^n + a_{n-1}b^{n-1} + \ldots\ldots + a_1 b + a_0 \pmod{n}$$

That is,

$$P(a) \equiv P(b) \pmod{n}$$

Proposition 10. If

$$a^x \equiv b^x \pmod{n}$$

and

$$a^y \equiv b^y \pmod{n}$$

then,

$$a^{(x,y)} \equiv b^{(x,y)} \pmod{n}$$

According to Bézout's identity we can find integers t, w such that

$$xt + yw = (x, y)$$

Using this, note that

$$a^{xt} \equiv b^{xt} \pmod{n}$$

And similarly,

$$b^{yw} \equiv b^{yw} \pmod{n}$$

Multiplying them,

$$a^{xt+yw} \equiv b^{xt+yw} \pmod{n}$$

Then,

$$a^{(x,y)} \equiv b^{(x,y)} \pmod{n}$$

We end this section. We shall see some theorems in congruences in the following section.

Note. Congruences are defined for negative exponent and fractions[1] too, but we keep that out of this discussion.

[1] That emerges the idea of *inverse modulo*, search in Wikipedia

3.3 Theorems On Congruences

Until now, we have just seen some propositions which actually follow from the definition of congruence. But now, we shall see some theorems related to congruence. First we shall discuss the famous *Fermat's Little Theorem*, *Euler's Totient Function* and then *Wilson's Theorem*.

3.3.1 Fermat's Little Theorem

Fermat's little theorem is actually the first non-trivial theorem and may be the most important theorem in congruence.

Theorem 1 (Fermat's Little Theorem)**.** *For any prime p and any integer a,*

$$a^p \equiv a \pmod{p}$$

It can be re-stated as

$$p|a^p - a$$

Note that if $p|a$, the proof is trivial. So, let's consider the case $p \not| a$ only. In this case we can divide the congruence by a,

$$a^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow p|a^{p-1} - 1$$

We shall prove the latter. First let's prove the following key fact related to *complete set of residue class* of p.

Claim 1. *For every $i \in \mathbb{Z}[p]$ and co-prime a to p, the remainder of ai is unique in $\mathbb{Z}[p]$.*

Proof. The proof is simple. We are sure that ai must give a remainder which is in $\mathbb{Z}[p]$. It is sure too that this remainder is unique. But we are not sure that there exists or not such j such that ai and aj gives the same remainder in $\mathbb{Z}[p]$. Assume, $i, j \in \mathbb{Z}[p]$

$$ai \equiv aj \pmod{p}$$

Divide it by a since $a \perp p$. Then

$$i \equiv j \pmod{p}$$

Equivalently,

$$p|i - j$$

But since both i and j are less than p,

$$|i - j| < p$$

Hence,

$$i - j = 0, i = j$$

Thus, the remainder of ai is unique for all $i \in \mathbb{Z}[p]$.

Apply this lemma for all i and then multiply. We shall get that

$$a \cdot 1 \cdot a \cdot 2 \cdots a \cdot (p-1) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

$$\Rightarrow a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Since p is co-prime to every numbers less than p, p is co-prime to their product as well.

$$(p, (p-1)!) = 1,$$

we can divide by $(p-1)!$. Then,

$$a^{p-1} \equiv 1 \pmod{p}$$

We have proven it.

□

Note. The converse of Fermat's little theorem is false. Remember problem 50 of divisibility section. There you proved

$$341 | 2^{341} - 2$$

But

$$341 = 11 \cdot 31$$

and so, 341 is composite. In such cases, when n is not a prime but

$$n | a^n - a.$$

n is called a *pseudo prime*.

If n is not prime but for all integers a,

$$a^n \equiv a \pmod{n}$$

then, n is called a *Carmichael number*.

Example. The smallest example of such numbers is $n = 561$. Because

$$561 | a^{561} - a$$

for all $a \in \mathbb{Z}$.

3.3.2 Euler's Totient Function Theorem

Euler's totient function theorem is also very important in number theory. In fact, this is the generalization of Fermat's little theorem. But for the description of this theorem, we need to know what *Euler's Function* is!

Definition 10 (Euler's totient function)**.** Euler's totient function $\varphi(n)$ is the number of positive integers less or equal to n and co-prime to n. In other words, $\varphi(n)$ is the number of elements in the set $\{1, 2, \ldots\ldots n\}$ which are co-prime to n. Sometimes it is called *totient function* or *phi function* too.

Example. If $n = 6$, there are 2 elements namely 1 and 5 which are co-prime to 6 in the set $\{1, 2, 3, 4, 5, 6\}$. So, $\varphi(6) = 2$. Similarly, $\varphi(12) = 4$.

Note. If $n = p$ a prime, then $\varphi(p) = p - 1$. Since every integer less than p is co-prime to p, this is obvious.

See some more examples yourself for convenience. Now come back to the theorem.

Theorem 2. *If $a \perp n$, then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof. The proof is much similar to the Fermat's one. Let, the co-prime numbers less than or equal to n are

$$r_1, r_2, \ldots\ldots, r_{\varphi(n)}$$

since there are $\varphi(n)$ elements. Then using the preceding claim and multiplying for $\varphi(n)$ times,

$$ar_1 \cdot ar_2 \cdots ar_{\varphi(n)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(n)} \pmod{n}$$

Since r_i's are co-prime to n for $1 \leq i \leq \varphi(n)$,

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Therefore, this theorem is also proved.

□

Corollary 13. If we set $n = p$, a prime, then we get

$$a^{\varphi(p)} \equiv 1 \pmod{p}$$

Which actually means that

$$a^{p-1} \equiv 1 \pmod{p}$$

That is, Fermat's theorem is a special case of Euler's theorem.

More On Phi Function In number theory, phi function is very necessary to learn. In this purpose, we discuss two very useful properties.

Definition 11 (Multiplicative Function)**.** A function f is called *multiplicative* if and only if for $m \perp n$ the condition,

$$f(mn) = f(m)f(n)$$

is satisfied.

Theorem 3. *φ is multiplicative. If $(m, n) = 1$,*

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Corollary 14. If $m_1, m_2, \ldots\ldots m_n$ are n pair wisely co-prime positive integers, then

$$\varphi(m_1 m_2 \cdot \cdots \cdot m_n) = \varphi(m_1)\varphi(m_2) \cdot \cdots \cdot \varphi(m_n)$$

Here we leave its proof. But you can make a sense by investigating and comparing the values of $\varphi(mn)$ and $\varphi(m)\varphi(n)$ for several m, n.[2]

But we shall prove the next theorem.

Theorem 4. *If p is a prime,*

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$$

Proof. First note the following counting of $\varphi(3^3)$. You may make a list of 27 numbers from 1 to 3^3. Then discard the numbers which are sharing a common factor with 3^3. You should notice that only the multiples of 3 are sharing a common factor. There are such 3^2 multiples. Thus, there will be $3^3 - 3^2$ numbers which are co-prime to 3^3. This argument certainly generalizes.

Note that p^α will share a factor with $p^{\alpha-1}$ numbers less than p^α. Thus, there will be total of $p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$ numbers co-prime to p^α. We may conclude that

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$$

□

Theorem 5. *If*

$$n = p_1^{a_1} p_2^{a_2} \cdot \cdots \cdot p_n^{a_n}$$

where $a_1, a_2, \ldots\ldots, a_n$ are positive integers and $p_1, p_2, \ldots\ldots, p_n$ are distinct primes then,

$$\varphi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdot \cdots \cdot p_n^{a_n-1} \cdot (p_1-1)(p_2-1)\cdots(p_n-1)$$

[2]Consider when $m \perp n$ and when $m \not\perp n$.

Proof. In fact, it follows from the two previous theorems. Since $p_1, p_2, \ldots\ldots p_n$ are distinct primes,

$$\varphi(p_1^{a_1} p_2^{a_2} \cdot \cdots \cdot p_n^{a_n}) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdot \cdots \cdot \varphi(p_n^{a_n})$$

Now, set

$$\varphi(p^a) = p^{a-1}(p-1)$$

And, the result follows.

□

Find $\varphi(n)$ for some large numbers like $100, 12^{100}, 56^9$ etc. This will help you to solve problems.

3.3.3 Wilson's Theorem

This is another important theorem. This is named after *Wilson* but it was originally proved by *Lagrange* and *Gauss* individually. Here, we shall discuss the proof of *Gauss* here.

If I ask you to count the remainder of 12! modulo 13, what shall you do? One approach is to multiply all numbers from 1 to 12. Then divide it by 13. But this is a stupid approach. Because you can't do the division if I ask you to do the same for 1979 and 1978!. So you must be tricky. Here the trick goes. Except the integers 1 and 12, we try to pair up them so that their product yields a remainder 1 upon division by 13.

$$12! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12$$

Note that,

$$2 \cdot 7 \equiv 1 \pmod{13}$$
$$3 \cdot 9 \equiv 1 \pmod{13}$$
$$4 \cdot 10 \equiv 1 \pmod{13}$$
$$5 \cdot 8 \equiv 1 \pmod{13}$$
$$6 \cdot 11 \equiv 1 \pmod{13}$$

Then

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \equiv 1 \pmod{13}$$

Then

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \equiv 1 \cdot 12 \pmod{13}$$

This means that

$$12! \equiv 12 \equiv -1 \pmod{13}$$

Equivalently,

$$12! + 1 \equiv 0 \pmod{13}$$

Here, note that we have 5 pairs. Because there were 12 positive integers in 12! and we didn't take 1 and 12 in the pairs. So there will be $\frac{13-3}{2} = 5$ pairs. For an arbitrary prime p, if such pairing is possible, then there would be $\frac{p-3}{2}$ pairs. Can we really generalize this result for all primes? If it is possible, we can conclude that :

Theorem 6. *For any prime p,*

$$(p-1)! \equiv -1 \pmod{p}$$

$$\Rightarrow p|(p-1)! + 1$$

Proof by Gauss. The proof is trivial for $p = 2$ as,

$$1! \equiv -1 \pmod{2}$$

So, consider p odd prime.

Actually, we are done if we can prove that for all

$$a \in \{2, 3, \ldots, p-2\}$$

there exists a unique

$$x \in \{2, 3, \ldots, p-2\}$$

such that

$$ax \equiv 1 \pmod{p}$$

Then we could pair up those a's with their corresponding x's and multiplying them out, we shall have that

$$2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \pmod{p}$$

$$\Rightarrow 1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-1) \equiv -1 \pmod{p}$$

$$\Rightarrow (p-1)! \equiv -1 \pmod{p}$$

$$\Rightarrow p|(p-1)! + 1$$

But are we sure that such x exist for all these a's at all? The answer is positive. Remember the corollary of Identity 5, from which since $p \perp a$, there exist integers x and y such that

$$ax + py = 1$$

Now,

$$ax + py \equiv ax \pmod{p}$$

$$\Rightarrow ax \equiv 1 \pmod{p}$$

The rest is to prove that this x is unique for a fixed a. This proof is same as the Fermat's one. So, I am leaving this. But note that $a \neq x$ because this would imply

$$a^2 \equiv 1 \pmod{p}$$

$$\Rightarrow p|(a+1)(a-1)$$

Since p is an odd prime, p won't divide both $a+1$ and $a-1$ because then we might have

$$p|(a+1) - (a-1) = 2$$

or $p = 2$ which is not true. Thus,

$$p|a+1 \text{ or } a-1$$

Also,

$$a < p, p \perp a-1$$

For this reason,

$$p|a+1$$

$$\Rightarrow a+1 \geq p$$

$$\Rightarrow a \geq p-1$$

But again, this is a contradiction since

$$a \in \{2, 3, \ldots\ldots p-2\}$$

□

3.4 Some Related Highly Used Ideas

Here are some congruences which we shall use while solving problems relating diophantine equations or something other. The equations which are to be solved in positive integers is called *diophantine equations.*

Example. $2^a + 3^b = 5^c$ is a diophantine equation if it is asked to solve in positive integers a, b, c.

3.4.1 Useful Congruences

Here are some very important congruences you may need to know. They are left as exercises. But while solving problems, they need not be proved. These congruences are specially useful for solving diophantine equations, or divisibility relational problems.

1. $x^2 \equiv \pm 1 \pmod 3$
2. $x^2 \equiv 0, 1 \pmod 4$
3. $x^2 \equiv 0, \pm 1 \pmod 5$
4. $x^2 \equiv 0, 1, 4 \pmod 8$
5. $x^2 \equiv 0, 4, -2 \pmod 9$
6. $x^3 \equiv 0, \pm 1 \pmod 7$
7. $x^3 \equiv 0, \pm 1 \pmod 9$
8. $x^4 \equiv 0, 1 \pmod{16}$
9. $x^5 \equiv 0, \pm 1 \pmod{11}$
10. $x^6 \equiv 0, 1 \pmod 9$
11. $x^6 \equiv 0, \pm 1 \pmod{13}$
12. $x^{10} \equiv 1 \pmod{11}$

Now, try to prove those. You should be able to prove them considering a complete set of residue class of the modulo taken. For example, we can prove the third congruence as below :

Every integer is one of the form

$$5n - 2, 5n - 1, 5n, 5n + 1, 5n + 2$$

Then square all of them and see the residues. You will get cyclically

$$-1, 1, 0, 1, -1$$

Thus, our third proposition was true and try the left ones.

3.4.2 Divisibility Issues

1. If two numbers are of same parity, then their difference is divisible by 2.

2. A number is divisible by 3 if and only if the sum of its digits is divisible by 3.

   Example. 15 is divisible by 3 since $1 + 5 = 6$ is divisible by 3.

3. A number is divisible by 4 if and only if the number formed by the last two digits is divisible by 4.

   Example. 10024 is divisible by 4.

4. A number is divisible by 5 if and only if its last digit is 5 or 0.

   Example. 55575 and 100 are divisible by 5.

5. A number is divisible by 7, if and only if the difference of two numbers formed by separating the last three digits and the rest number is divisible by 7.

   Example. 2401 is divisible by 7 because $401 - 2 = 399 = 7 \cdot 57$ which is divisible by 7.

6. A number is divisible by 8 if and only if the number formed by the last three digits are divisible by 8.

   Example. 5512 is divisible by 8 because 512 is divisible by 8.

7. A number is divisible by 9 if and only if the sum of its digits is divisible by 9.

   Example. 3456 is divisible by 9 since $3 + 4 + 5 + 6 = 18$, divisible by 9.

8. A number is divisible by 11 if and only if the difference of sums between the odd positioned digit and even positioned digit is divisible by 11.

   Example. 121341 is divisible by 11 since $1 + 1 + 4 - (2 + 3 + 1) = 0$, divisible by 11.

You may wonder that why these are put in congruence section. Because they are easily solved with congruences. They are very often used in problems.

Part II

Problems

Chapter 4

Problems In Divisibility

The problems that have solutions should come first.

4.1 Problems With Solutions

Gaining a good experience in divisibility requires a good practice. So, to have mastered in this section, you must solve enormous problems. In this purpose, I have put a huge number of problems. Some of them have solutions, other don't. Those are left as exercises. Let's start our journey.

1. Find all $n \in \mathbb{N}$ such that

$$n|2n+1$$

Solution. Given,

$$n|2n+1$$

But,

$$n|2n$$

So by #7 of divisibility properties,

$$n|(2n+1)-(2n)=1$$

Thus, the only value for $n=1$.

Remark 3. Alternatively,

$$\begin{aligned} & n|2n+1 \\ \Rightarrow & \frac{2n+1}{n} \text{ is a positive integer} \\ \Rightarrow & \frac{2n+1}{n} = 2+\frac{1}{n} \text{ is a positive integer} \end{aligned}$$

which implies that $\frac{1}{n}$ is a positive integer. Thus, $n = 1$.

You may often do this. But when the fractions are too ugly to deal with in this approach, then divisibility relations come to the rescue. So, try to make the sense when and how you need to use divisibility. For this, of-course you must have more practice.

2. Find all primes p such that $17p + 1$ is a prime.

Solution. If $p > 2$, obviously p odd. Otherwise, p would be divisible by 2. But then $17p$ is odd and $17p + 1$ is even, so not prime. But if $p = 2$, then $17p + 1 = 35$ which is not a prime. So, no such prime exists.

3 (Divisional Olympiad, Dhaka, 2010)**.** Find all positive integers greater than 1 which divides both $N + 4$ and $N + 12$.

Solution. Assume that,

$$d|N + 4$$

$$d|N + 12$$

Then, $d|8$ and since $d > 1$, $d = 2, 4, 8$.

4. Find all $n \in \mathbb{N}$ such that $n + 2|5n + 6$

Solution.

$$n + 2|5n + 6$$

But,

$$n + 2|5n + 10$$

Combining,

$$n + 2|4$$

That is, $n + 2$ is a divisor of 4. Since $n + 2 \geq 3$, it follows that $n + 2 = 4$. Then $n = 2$.

Note. We are always trying to eliminate n from the divisibility relation so that we get only a numerical value. You may also notice that, for doing this we multiply by some factors and add or subtract and some more operations are done. This is important to realize that why we are doing so, and why we are multiplying by that factor. Try to solve them using another factors. See next problems for more approaches how to remove the variables from these relations.

5. Find all $m \in \mathbb{N}$ so that

$$3m + 1|6m + 8$$

Solution.

$$3m+1|6m+2, 6m+8$$
$$\implies 3m+1|6$$

Since $3m+1 \geq 4$,

$$3m+1 = 6$$

But this is not possible. So there exist no such m.

6. Find all n that satisfies the relation:

$$7n+1|8n+55$$

Solution. This time we are going to see a general approach. By the time, probably you have noticed that we need the coefficients of n equal on both sides so that after subtraction, they cancel each other. So,

$$7n+1|8(7n+1) = 56n+8$$

Again,

$$7n+1|8n+55|56n+385$$
$$\Rightarrow 7n+1|377$$

Now, our task is to factorize 377. So, let's use the property #11 of divisibility.

We need to concentrate on primes less or equal to $\sqrt{377}$ only. Note that

$$\sqrt{377} < \sqrt{400} = 20$$

So, check with primes $3, 5, 7, 11, 13, 15, 17, 19$ only. This easy check shows that

$$13|377, 377 = 13 \cdot 19$$

Then $7n+1 = 17$ or 19 or 377. No case gives a valid result. So, no solution.

7. Every primes greater than 3 are of the form $6k \pm 1$.

Solution. Notice, we can represent any integer in one of the form $6k, 6k-1, 6k-2, 6k+1, 6k+2, 6k-3$.
But $6k-3, 6k+2, 6k-2, 6k-2$ are never primes (except $6k-3=3$ for $k=1$, that's why we discarded 3 at first). So, if a positive integer is a prime, then it must be of the form $6k \pm 1$.

8. a and b are positive integers and x, y are integers such that,

$$ax + by = 1$$

Prove that

$$(a,b) = 1, (a,y) = 1, (x,y) = 1, (x,b) = 1.$$

Solution. Let $(a, b) = g, a = ga', b = gb'$ where $(a', b') = 1$.Then

$$g(a'x + b'y) = 1$$

$$\Rightarrow g|1, g = 1$$

The other cases are exactly the same.

Corollary 15. The converse of Identity 5 is also true.

9. Find the maximum value of x such that $x + 25|(x + 2)^2$

Solution.

$$x + 25|x^2 + 4x + 4$$

$$x + 25|(x + 25)(x - 25) = x^2 - 625$$

Subtracting yields,

$$x + 25|4x + 629$$

and also

$$x + 25|4x + 100$$

Then again subtract to get

$$x + 25|529$$

Since,

$$x + 25 \geq 529$$

the maximum value of

$$x_{max} = 529 - 25 = 504$$

10 (Secondary Special Camp 2010 Number Theory Problem 1(b))**.** Find all positive integers d such that d divides n^2+1 and $(n+1)^2+1$ for some natural n.

Solution.

$$d|n^2 + 1, n^2 + 2n + 2$$

$$\Rightarrow d|2n + 1$$

Again, $d|2n + 1$ Moreover,

$$2n + 1|4n^2 - 1$$

$$n^2 + 1|4n^2 + 4$$

Hence,

$$d|4n^2 + 4$$

Finally, we have $d|5$ i.e. $d = 1, 5$.

11. Prove that

$$(a, bc) = (a, (a, b) \cdot c)$$

Solution. Let $(a, b) = g, a = ga', b = gb'$ where $(a', b') = 1$.
Then,

$$(a, bc) = (ga', gb'c)$$

Using *gcd* property #9, we have

$$(a, bc) = g(a', b'c)$$

Since $a' \perp b'$, using #15,

$$(a, bc) = g(a', c)$$

On the other hand from divisibility property #9,

$$(a, (a, b) \cdot c) = (ga', gc) = g(a', c)$$

Of-course, both of them are equal.

12 (IMO - 1959,1)**.** Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible.[1]

Solution. From the definition of irreducible fraction, it is clear that it is sufficient to prove that

$$(21n + 4, 14n + 3) = 1$$

And we shall solve this in several ways to see some beautiful applications of divisibility.

1. Assume $(21n + 4, 14n + 3) = g$. Using *gcd* property #1,

$$g|21n + 4, g|14n + 3$$

Note that,

$$21n + 4|2(21n + 4) = 42n + 8$$
$$14n + 3|3(14n + 3)$$

Then

$$g|42n + 8, 42n + 9 \Longrightarrow g|(42n + 9) - (42n + 8) = 1, g = 1$$

Question. Why did we multiply the relations by 2 or 3 here. Which should drive you to do so?

[1] A fraction is *irreducible* if we can't remove a common factor from the denominator and the numerator.

2. For this solution, let's use Euclidean algorithm.

$$(14n+3, 21n+4) = (14n+3, 7n+1)$$

after subtracting $14n+3$ from $21n+4$. Again,

$$(7n+1, 14n+3) = (7n+1, 7n+2) = (7n+1, 1) = 1$$

Thus, we are done.

3. This time we shall use Identity 5. According to Corollary 6, the proof will be complete if we can find integers x, y so that

$$(14n+3)x + (21n+4)y = 1$$

Now just note that :

$$3(14n+3) - 2(214n+4) = 1$$

Remark 4. All three proofs are equivalent. For instance, see that while we multiply by $3, 2$ in solution 1, we actually did the same in solution 3.

13 (Euler)**.** Show that $2^{32}+1$ is divisible by 641.

Solution. First note that :

$$641 = 16 + 625 = 2^4 + 5^4$$

$$641 = 640 + 1 = 5 \cdot 128 + 1 = 5 \cdot 2^7 + 1$$

It is very easy to note:

$$a+1 | a^4 - 1$$

After setting $a = 5 \cdot 2^7$, we have

$$641 | 5^4 \cdot 2^{28} - 1$$

Furthermore,

$$2^4 + 5^4 | 2^{32} + 5^4 \cdot 2^{28}$$

Now a subtraction shows that,

$$641 | 2^{32} + 1$$

Remark 5. The numbers of the form $2^{2^n}+1$ is called the *Fermat's Number* and the n^{th} Fermat's number is denoted by F_n.

$$F_n = 2^{2^n}+1$$

Fermat noticed that some first numbers of this form are primes and conjectured that F_n are always primes. Euler first disproved Fermat showing the counter example above that

$$641|F_5$$

14. Prove that for all odd $k \in \mathbb{N}$,

$$1+2+\ldots\ldots+n|1^k+2^k+\ldots\ldots+n^k$$

Solution. You should know that,

$$1+2+\ldots\ldots+n = \frac{n(n+1)}{2}$$

If you don't know try to prove it yourself. It can be proved in many ways.

Now, it suffices to prove that

$$n(n+1)|2(1^k+2^k+\ldots\ldots+n^k)$$

Remember Corollary 3 in *gcd* properties. We are done if we can prove the following two independently :[2]

$$n|2(1^k+2^k+\ldots\ldots+n^k)$$

$$n+1|2(1^k+2^k+\ldots\ldots+n^k)$$

Again re-call Corollary 6,

$$n = 1+(n-1)|1^k+(n-1^k), 2^k+(n-2)^k, \ldots$$

This shows the first part. For the second part, note that

$$n+1|1^k+n^k, 2^k+(n-1)^k, \ldots$$

Therefore, the second part is also true.

15. Find the maximum value of n such that $\frac{n^3+10}{n+10}$ is a positive integer.

[2]why is it sufficient?

Solution. From the problem statement,

$$n + 10 | n^3 + 10$$

Also,

$$n + 10 | n^3 + 1000$$

Thus,

$$n + 10 | 990$$

implying that,

$$n_{max} = 980$$

16 (IMO - 1964,1)**.** Prove that $n^4 + 4^n$ is always composite for $n > 1$.

Solution. If n is even, obviously $n^4 + 4^n$ is an even number greater than 2, hence divisible by 2 at least.

Now, consider $n > 1$ odd. Let

$$n = 2a + 1$$

We can re-write

$$n^4 + 4^n = n^4 + 4^{2a+1} = n^4 + 4 \cdot (2^a)^4$$

This is of the form $a^4 + 4b^4$ which is composite by Corollary 4.

17. Find all $n \in \mathbb{N}$ such that

$$5n + 1 | n^6 + n^4$$

Solution.

$$5n + 1 | n^4(n^2 + 1)$$

but

$$n \perp 5n + 1$$

So from #19 of divisibility we have

$$n^4 \perp 5n + 1$$

giving,

$$5n + 1 | n^2 + 1 \Rightarrow 5n + 1 | n^2 - 5n = n(n - 5)$$

Again,

$$n \perp 5n + 1$$

and so

$$5n + 1 | n - 5$$

It is evident that the absolute value of $n - 5$ is less than $5n + 1$. Therefore,

$$n - 5 = 0 \Longrightarrow n = 5$$

18. When is $n^5 + n^4 + 1$ a prime?

Solution. Let's try to factorize $n^5 + n^4 + 1$.

Note that,

$$n^5 + n^4 + 1 = (n^2 + n + 1)(n^3 - n + 1)$$

We need

$$n^3 - n + 1 = 1$$

This produces the solution $n = 1$.

Question. What should lead us to this factorization?

19. Find all $n \in \mathbb{N}_0$ such that

$$2^n + n | 8^n + n$$

Solution. Does the fact $8 = 2^3$ suggest you anything?

Yes, it suggests us to use Corollary 5.

$$a + b | a^3 + b^3$$

Then,

$$2^n + n | (2^n)^3 + n^3 = 8^n + n^3$$

and also

$$2^n + n | 8^n + n$$

These two yields

$$2^n + n | n^3 - n$$

Now, let's search for n such that

$$2^n + n > n^3 - n$$

Because then we can conclude

$$n^3 - n = 0$$

which is not possible except $n = 0, 1$. A quick search shows that the convenient choice for n is 10. Since then

$$1034 > 990$$

What can be the way to prove that

$$2^n + n > n^3 - n$$

for $n > 9$? It is *induction*. If you don't know about induction, consult with Wikipedia.

The base case $n_0 = 10$ is true as we have shown before. Let be true $n = k$ for some $k \in \mathbb{N}, k > 10$. Then we have

$$2^k + k > k^3 - k$$

Now let's prove its truth for $n = k + 1$.

Note that

$$(k+1)^3 - (k+1) = k^3 + 3k^2 + 2k$$

The inequality is reduced to

$$2^{k+1} + k + 1 > k^3 + 3k^2 + 2k$$

Again, notice

$$2 \cdot 2^k + k + 1 = 2(2^k + k) - k + 1 > 2(k^3 - k) - k + 1 = 2k^3 - 3k + 1$$

We are done if we can show that

$$2k^3 - 3k + 1 > k^3 + 3k^2 + 2k$$

Or equivalently,

$$k^3 + 1 > k^3 > 3k^2 + 5k \Rightarrow k^2 > 3k + 5$$

Which is true since

$$k^2 = k \cdot k > 10k > 3k + 5$$

Thus we need to check only the values of

$$0 \leq n \leq 9$$

Checking shows that the only solutions are

$$n \in \{1, 2, 4, 6\}$$

20 (Spanish Mathematical Olympiad-1996)**.** If

$$\frac{a+1}{b} + \frac{b+1}{a}$$

is a positive integer, then

$$a + b \geq (a, b)^2$$

Solution.

$$\frac{a+1}{b}+\frac{b+1}{a}=\frac{a^2+b^2+a+b}{ab}$$

Let $(a,b)=d, a=da', b=db'$ with $(a',b')=1$.Then,

$$ab|a^2+b^2+a+b$$

And also

$$d^2|a^2, d^2|b^2$$

implying that,

$$d^2|a^2+b^2$$

Again,

$$d^2|ab$$

$$d^2|ab|a^2+b^2+a+b$$

$$\Rightarrow d^2|a+b$$

$$\Rightarrow d^2\leq a+b$$

21. Find all natural n that

$$1000^m-1|1978^m-1$$

Solution.

$$1000^m-1|1978^m-1000^m=2^m(989^m-500^m)$$

But

$$(2^m,1000^m-1)=1$$

And hence,

$$1000^m-1|989^m-500^m$$

Note the following contradicting inequality

$$989^m-500^m<1000^m-1$$

22 (IMO - 1998, Problem 4)**.** Find all pairs of positive integers (a,b) such that

$$ab^2+b+7|a^2b+a+b$$

Solution. We use divisibility relations to solve this problem.

$$ab^2 + b + 7 | a^2b + a + b$$

So,

$$ab^2 + b + 7 | b(a^2b + a + b) = a^2b^2 + ab + b^2$$

Also

$$ab^2 + b + 7 | a(ab^2 + b + 7) = a^2b^2 + ab + 7a$$

Thus,

$$ab^2 + b + 7 | b^2 - 7a \text{ or } 7a - b^2$$

If $b = 1$, then

$$\begin{aligned} & a + 8 | 7a - 1 \\ \Rightarrow\ & a + 8 | 7a + 56 \\ \Rightarrow\ & a + 8 | 57 \end{aligned}$$

Since $a + 8 > 3$ and $57 = 3 \cdot 19$. We have

$$a + 8 = 19, a = 11 \text{ or } a + 8 = 57, a = 49$$

Now, let's assume $b > 1$. Then the absolute value of $b^2 - 7a$ is less than $ab^2 + b + 7$. So,

$$\begin{aligned} & b^2 - 7a = 0 \\ \Rightarrow\ & b^2 = 7a \\ \Rightarrow\ & 7 | b \end{aligned}$$

Let $b = 7c$. This gives $a = 7c^2$. Check that $(a, b) = (7c, 7c^2)$ is a solution indeed.

Therefore all solutions are given by,

$$(a, b) = (11, 1), (49, 1), (7c^2, 7c)$$

23. Count $(x^2 - x + 1, x^2 + x + 1)$

Solution. Let,

$$g = (x^2 - x + 1, x^2 + x + 1)$$

Since $x^2 - x + 1$ and $x^2 + x + 1$ both odd, g is odd too.

$$g | x^2 - x + 1$$

$$g | x^2 + x + 1$$

Subtracting,

$$g|2x$$

Since g odd,

$$g|x|x^2 - x$$

$$\Rightarrow g|x^2 - x + 1 - (x^2 - x) = 1$$

Thus, $g = 1$.

24. Find all integer solutions to

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$$

Solution. Re-write the equation as

$$z = \frac{xy}{x+y}$$

We need

$$x + y|xy$$

Let's assume

$$(x, y) = g, x = gx', y = gy'$$

Here,

$$(x', y') = (x', x' + y') = (y', x' + y') = 1 \qquad (*)$$

Now,

$$z = \frac{gx'y'}{x' + y'}$$

From $(*)$,

$$x' + y'|g$$

Let $g = (x' + y')k$. Then,

$$z = x'y'k, x = (x' + y')kx', y = (x' + y')ky'$$

25. Find all m such that $2^{m+1} - m^2$ is a prime.

Solution. If m even, obviously $2^{m+1} - m^2$ is an even integer greater than 2, so not prime. Therefore, m odd.

Let $m = 2k + 1$. Then

$$2^{m+1} - m^2 = (2^{k+1} + m)(2^{k+1} - m)$$

The latter implies that

$$2^{k+1} - 2k - 1 = 1$$
$$\implies 2^k - k = 1$$

If $k > 1$, then

$$2^k - k > 1$$

So, $k = 0, 1$. Then,

$$m = 1, 3$$

26. Prove that if,

$$a^m - 1 | a^n - 1$$

then $m|n$.

Solution. Here are two solutions.

1. Set $b = 1$ in the Identity 6. Then applying #20,

   $$(a^m - 1, a^n - 1) = a^{(m,n)} - 1 = a^m - 1$$

   So, $(m, n) = m$ i.e. $m|n$.

2. $$a^m - 1 | a^n - 1$$
   $$\Rightarrow a^m - 1 | a^n - a^m = a^m(a^{n-m} - 1)$$

   Certainly,

   $$a^m - 1 \perp a^m$$

   So,

   $$a^m - 1 | a^{n-m} - 1$$

   Again,

   $$a^m - 1 | a^{n-m} - a^m = a^m(a^{n-2m} - 1)$$
   $$\Rightarrow a^m - 1 | a^{n-2m} - 1$$

   Let $n = mq + r, r < m$. Then repeating this process,

   $$a^m - 1 | a^{n-mq} - 1$$
   $$\Rightarrow a^m - 1 | a^r - 1$$

   But

   $$a^r - 1 < a^m - 1$$

   So,

   $$a^r - 1 = 0 \Rightarrow r = 0$$

   Then $n = mq$ i.e. $m|n$.

27 (Masum Billal)**.** Construct a non-decreasing sequence a_i of positive integers (i.e. $a_{i+1} \geq a_i$) such that

$$(a_{i+2}, a_{i+1}) = [a_i, a_{i-1}]$$

Solution. We will show that $a_i = a$ satisfies the given condition where a is a constant positive integer.

It suffices to show that

$$a_{i+1} = a_i \text{ for all } i$$

We already know that

$$a_i | [a_i, a_{i-1}]$$

Also,

$$(a_{i+1}, a_{i+2}) | a_{i+1}$$

Thus,

$$a_i | [a_i, a_{i-1}] = (a_{i+1}, a_{i+2})$$

$$a_i | a_{i+1}$$

$$(a_{i+1}, a_{i+2}) = [a_i, a_{i-1}]$$

It immediately follows that,

$$a_{i+1} = a_i$$

as we desired to show.

28 (Romanian Mathematical Olympiad-2002)**.** Let n be an even positive integer. Find all co-prime positive integers a and b such that

$$a + b | a^n + b^n$$

29. Since n even, from the identity

$$a^2 - b^2 = (a + b)(a - b)$$

we have

$$a + b | a^n - b^n$$

Also, we have

$$a + b | a^n + b^n$$

Thus,

$$a + b | 2a^n$$

But $a \perp a+b$,[3] so,

$$a+b|2$$

Hence,

$$a+b=2$$

giving solution

$$a=1, b=1$$

4.2 Problems Without Solutions

30. The difference of two odd numbers is divisible by 2 but not by 4. Prove that their sum is divisible by 4.

31. Prove that if the sum of two numbers is a prime, then they must be co-prime to each other.

32. Find all a such that

$$a+23|(a+1)^2$$

33. Prove that for all odd $n \in \mathbb{N}$,

$$n^2|1^3+2^3+\ldots\ldots+n^3$$

34. Prove that if p is a Sophie Germain prime,[4] then p and q must be of the form $6n-1$.

35. Prove that the square of an odd integer leaves a remainder 1 upon division by 8.

36. Prove that if $m|n$,

$$a^m-1|a^n-1$$

37. Find all $a, m, n \in \mathbb{N}$ such that

$$a^m-1|a^n+1$$

38. Decide if a number ending with some zero's and starting with some two's is a perfect square or not ¿

39. Prove that for a prime $p>3$,

$$24|p^2-1$$

[3]make sure you understand why it is so!

[4]A prime p is called to be *Sophie Germain Prime* if $q=2p+1$ is also a prime. For example, 3 is such a prime since $2 \cdot 3+1=7$, a prime.

40. Is #18 of *gcd* true for more than two numbers?

41. Find all pairs of $(a, b) \in \mathbb{N}$ such that

$$2^a - 1 | 2^b + 1$$

42. Find all pairs of $(a, b, c) \in \mathbb{N}$ such that

$$2^a - 1 | 2^b + 2^c + 1$$

43. Is $2^{2^{2011}+2011}$ composite?

44. Find the maximum n such that n consecutive integers are pair-wisely co-prime.

45. If $2n + 1$ and $3n + 1$ are squares, prove that $8|n$

46. If $8^n + 1$ is a prime, prove that n must be a power of two. Generalize this!

47. Find all positive integer pairs of (a, b) such that

$$\frac{b}{a} + \frac{a}{b}$$

is a positive integer.

48. Complete the proof of Bézot's Identity (Identity 5).

49. Prove that for all odd $n \in \mathbb{N}$,

$$n | 1^n + 2^n + \ldots\ldots + (n-1)^n + n^n$$

50. Decide if N a prime, where

$$N = 4^{449} + 81.$$

51. Prove that the sum of divisors of a perfect square is odd.

52. Prove that the diophantine equation

$$12x + 54y = 65464$$

has no solutions in integers.[5]

[5]More generally, prove that if

$$ax + by = c$$

then the equation has solutions in integers if and only if

$$(a, b) | c$$

Prove it!

53. If

$$(a, b) + [a, b] = a + b$$

then one of a, b divides another.

54. Prove that

$$341|2^{341} - 2$$

55. Prove that there exists an infinite pairs of positive integer pairs (a, b) such that

$$a + b^2|a^3 + b^3$$

56. Find an infinite quadruple (a, b, c, d) such that

$$ac - bd = 1$$

and they are pair-wisely co-prime.

57. The numbers of the form $2^n - 1$ are called *Mersenn Numbers*.

$$M_n = 2^n - 1$$

Prove that if M_n is a prime, then n is a prime too.

58. Find all pairs of $(a, b) \in \mathbb{N}$ so that

$$ab|a^3 + b^3$$

59. Decide if we can find infinitely many pairs of (a, b) such that

$$ab + 1|a^2 + b^2 + 3$$

60. If $m = 4a + 3$ is divisible by 11, then what is the remainder of a^4 upon division by 11?

61. Prove that there exists an infinite pairs of positive integers (a, b) such that

$$ab + 1|a^2 + b^2$$

62. Prove that there exists infinitely many $(x, y) \in \mathbb{N}$ such that

$$xy + 1|x^2 + y^2 + 1$$

63. Prove that there exist an infinite pairs of $(x, y) \in \mathbb{N}$ such that

$$x + y|x^2 + y^2 + x + 1$$

64. Let a be an odd integer. Prove that

$$2^{k+1}|a^{2^k}-1$$

65. Find all natural solutions to the equation

$$p^a+p^b=p^c$$

where p is a prime.

66. Find an infinite (a,b,c) such that

$$a+b+c|3abc$$

67. For any prime factor p of n, if

$$p|\frac{n}{p}-1$$

prove that, n is square-free.[6]

68. Find all primes p such that $p-4$ is a perfect 4^{th} power[7].

69. Find all $n\in\mathbb{N}$ such that

$$3|n\cdot 2^n-1$$

70. Find all odd n such that

$$n|3^n+1$$

71. Prove that the product of two numbers of the form a^2+ab+b^2 is of the same form.

72 (Samin Riasat)**.** Show that if a number has k digits and its repeat[8] number is a perfect square, then 10^k+1 is never square-free.[9]

73. Prove that both 2^n-1 and 2^n+1 can't be prime at a time i.e. if one of them is prime, then the other is composite.

74. Does there exist an infinite positive integer n such that

$$n|2^n+1$$

75 (IMO 1990, 3)**.** Find all positive integers such that:

$$n^2|2^n+1$$

---

[6]A number is called *square-free* if it has no square factor i.e. it has no divisor which is a perfect square. For example, $n=12$ is not square-free whereas $n=78$ is.

[7]A number is called *perfect k-th power* if it can be expressed as n^k for $n,k>1$.

[8]The *repeat* of a number is called the number we get writing the number besides the original number. For example, the repeat of 123 is 123123.

[9]The original problem was:

> Find a repeat number which is a perfect square(if exists).

Chapter 5

Problems In Congruence

5.1 Problems With Solutions

76. What is the remainder if 2^{2011} is divided by 7.

Solution. From theorem 1, since $2 \perp 7$,

$$2^6 \equiv 1 \pmod 7$$

$$\Rightarrow 2^{6 \cdot 335} \equiv 1 \pmod 7$$

$$\Rightarrow 2^{2010} \equiv 1 \pmod 7$$

$$\Rightarrow 2^{2011} \equiv 2 \pmod 7$$

Thus the remainder is 2.

77. What is the last digit of 3^{81}.

Solution. First note that the last digit of a number is nothing but the remainder of the number upon division by 10. Now, the task is to determine the remainder of 3^{81} when divided by 10.

We give two solutions.

1. See the remainders when the powers of 3 are divided by 10.

$$3^1 \equiv 3 \pmod{10}$$

$$3^2 \equiv 9 \pmod{10}$$

$$3^3 \equiv 7 \pmod{10}$$

$$3^4 \equiv 1 \pmod{10}$$

$$3^5 \equiv 3 \pmod{10}$$

. . . . . .

It is obvious that from now, the sequence of last digit is periodic. The sequence is

$$3, 9, 7, 1, 3, \ldots$$

Since the period is 4, it is enough to find the last digit of the exponent modulo 4.

Therefore,

$$3^{81} \equiv 3^1 \equiv 3 \pmod{10}$$

Then, the last digit is 3.

2. Apply Euler's totient theorem.

$$3^{\varphi(10)} \equiv 1 \pmod{10}$$

$$\Rightarrow 3^4 \equiv 1 \pmod{10}$$

$$\Rightarrow 3^{80} \equiv 1 \pmod{10}$$

$$\Rightarrow 3^{81} \equiv 3 \pmod{10}$$

Thus the last digit is 3, as we deduced before.

Note. The latter solution shows why the sequence is periodic and the period is 4.

You can generalize that if $a \perp 10$, then the sequence of the last digit is periodic with a period 4.

78. Prove that

$$561 | a^{561} - a$$

Solution. Note that

$$561 = 3 \cdot 11 \cdot 17$$

Now, again,

$$561 | a(a^{560} - 1)$$

If any of 3, 11, or 17 is not co-prime to a, then it is of-course divisible by 3, 11 or 17. Else, we have

$$a^2 \equiv 1 \pmod{3}$$

$$\Rightarrow a^{560} \equiv 1 \pmod{3}$$

For 11,

$$a^{10} \equiv 1 \pmod{11}$$

$$\Rightarrow a^{560} \equiv 1 \pmod{11}$$

Similarly, since

$$17 - 1 = 16 | 560$$

we can say,

$$a^{560} \equiv 1 \pmod{16}$$

It turns out that,

$$3, 11, 17 | a^{560} - 1$$

Since $3, 11, 17$ are co-prime to each other from Corollary 2,

$$3 \cdot 11 \cdot 17 = 561 | a^{560} - 1$$

Note. 561 is the first Carmichael number.

79. Prove that for all $a, b \in \mathbb{Z}$ and p prime,

$$p | ab^p - ba^p$$

Solution. If one of a, b is divisible by p, we are done. If not, note that

$$a^{p-1} \equiv 1 \pmod{p}$$

and

$$b^{p-1} \equiv 1 \pmod{p}$$

Then from proposition 5,

$$a^{p-1} \equiv b^{p-1} \pmod{p}$$

Multiplying both sides by ab,

$$a^p b \equiv ba^p \pmod{p}$$

$$\Rightarrow p | ab^p - ba^p$$

80. Is $2010^{2010} - 1$ divisible by 2011?

Solution. The answer is positive. In fact, it is straight forward from theorem 1. But how are you sure that 2011 is a prime? Yes, use the same idea we used in problem 6 to decompose 377 in primes. But you need to check for primes upto 43 because

$$45^2 = 2025 > 2011$$

So the nearest prime will be 43. Do this yourself. And since

$$2011 \perp 2010$$

conclude that

$$2011 | 2010^{2010} - 1$$

81. Find all integers x, y, z such that

$$15x^2 - y^2 = 1234$$

Solution. What should strike you? This equation has no solutions! But how to prove that?

Re-call item 1 in section 2.4. This will show you

$$y^2 \equiv 0 \text{ or } -1 \pmod 3$$

Now, **take modulo 3 in the equation**. We get

$$15x^2 - y^2 \equiv 1234 \equiv 1 \pmod 3$$

$$\Rightarrow -y^2 \equiv 1 \pmod 3$$

$$\Rightarrow y^2 \equiv -1 \pmod 3$$

Since both sides are equal, we must have the same remainder upon division by the same number in the equation. But we have found a fact which is not satisfied by any integers. Therefore, no solutions.

Remark 6. It is a common tactic to use congruence on integer equations to derive a contradiction or informations about the properties of integers (such as **parity**) satisfying that particular equation. But there is no rule which modulo should be taken for an equation. This must be gained by your thinking power and more practice. This is a very popular idea of solving problems. But don't think that we don't have solutions in all cases. You have to be experienced for solving such equations.

82. Prove that for a prime $p > 3$,

$$p | (p-2)! - 1$$

Solution. From theorem 6,

$$(p-1)! \equiv 1 \pmod{p}$$

$$\Rightarrow (p-1)! \equiv (p-1) \pmod{p}$$

$$\Rightarrow (p-2)! \equiv 1 \pmod{p}$$

We can divide by $p-1$ since $p \perp p-1$.

83. Prove the fact 6 in section 3.4.1 without using the idea of complete set of residues.

Solution. If $7|x$, then

$$x^3 \equiv 0 \pmod{7}$$

Else, we have $7 \not| x$ and

$$x^6 \equiv 1 \pmod{7}$$

Then we can take square root on the congruence. That is,

$$x^3 \equiv \pm 1 \pmod{7}$$

If p is a prime and

$$a^2 \equiv b^2 \pmod{p}$$

then

$$a \equiv \pm b \pmod{p}$$

Remark 7. We could take square root on this congruence.

Explanation :

$$7|x^6 - 1 = (x^3+1)(x^3-1)$$

7 can't divide both of x^3+1 and x^3-1 because that would imply

$$7|(x^3+1) - (x^3-1) = 2$$

a contradiction! So, either x^3+1 or x^3-1 is divisible by 7.

84. Prove that

$$7|2222^{5555} + 5555^{2222}$$

Solution. Since 7 is a prime, Fermat's theorem is an obvious approach.

Note that,

$$2222 \equiv 3 \pmod{7}$$

$$5555 \equiv 4 \pmod{7}$$

Also,

$$\varphi(7) = 6$$

So,

$$\begin{aligned} 4^6 &\equiv 1 \pmod 7 \\ \Rightarrow 4^{2220} &\equiv 1 \pmod 7 \\ \Rightarrow 4^{2222} &\equiv 4^2 \pmod 7 \\ \Longrightarrow 5555^{2222} &\equiv 2 \pmod 7 \end{aligned}$$

And,

$$\begin{aligned} 3^6 &\equiv 1 \pmod 7 \\ \Rightarrow 3^{5550} &\equiv 1 \pmod 7 \\ \Rightarrow 3^{5555} &\equiv 3^5 \pmod 7 \\ \Rightarrow 2222^{5555} &\equiv 5 \pmod 7 \end{aligned}$$

Then

$$2222^{5555} + 5555^{2222} \equiv 2 + 5 \equiv 0 \pmod 7$$

85. Find all positive integer solutions to :

$$a^2 + b^2 = 1234567899091$$

Solution. There is a large number in the right side. Nothing to be afraid, because actually it has nothing to do with this problem. In fact, this equation has no solutions. So, what should be our approach?

Remember item 2 of section 2.4 . We have

$$a^2 \equiv 0, 1 \pmod 4$$

and

$$b^2 \equiv 0, 1 \pmod 4$$

Thus,

$$a^2 + b^2 \equiv 0, 1, 1 + 1 = 2 \pmod 4$$

But $a^2 + b^2$ can never be $3 \pmod 4$. So, we have found a contradiction!

86. Find all integers $a_1, a_2, \ldots\ldots, a_{14}$ such that

$$a_1^4 + a_2^4 + \ldots\ldots + a_{14}^4 = 1599$$

Solution. When you see the power 4, you should re-call item 8. Also, the number 1599 suggests the modulo 16. This modulo will yield a remainder of left side which ranges from 0 to 14 since each of $a_1^4, a_2^4, \ldots\ldots, a_{14}^4$ gives a remainder 0 or 1. But

$$1599 \equiv 15 \pmod{16}$$

Since we can never attain 15 in left side, it is a clear contradiction.

87. Let,

$$a_n = 6^n + 8^n$$

Find the remainder when a_{49} is divided by 49.

Solution. Note that both 6 and 8 are co-prime to 49 and

$$\varphi(7^2) = 7 \cdot (7-1) = 42$$

so,

$$6^{42} \equiv 1 \pmod{49}$$

and

$$8^{42} \equiv 1 \pmod{49}$$

Now, we have to count 6^7 and 8^7 modulo 49. Be *tricky*. One approach is to count 6^7 and 8^7 directly and then divide it by 49. But we can do it more easily.

$$\begin{gathered}
6^2 \equiv -13 \pmod{49} \\
\Rightarrow 6^4 \equiv 13^2 \equiv 169 \equiv 22 \pmod{49} \\
\Rightarrow 6^4 \cdot 6^2 \equiv 22 \cdot (-13) \pmod{49} \\
\Rightarrow 6^6 \equiv 8 \pmod{49} \\
\Rightarrow 6^7 \equiv 48 \equiv -1 \pmod{49} \\
\Rightarrow 6^{49} \equiv -1 \pmod{49}
\end{gathered}$$

On the other hand,

$$\begin{gathered}
8^2 \equiv 15 \pmod{49} \\
\Rightarrow 8^4 \equiv 15^2 \equiv -20 \pmod{49} \\
\Rightarrow 8^4 \cdot 8^2 \equiv 15 \cdot (-20) \equiv -6 \pmod{49} \\
\Rightarrow 8^7 \equiv (-6) \cdot 8 \equiv 1 \pmod{49} \\
\Rightarrow 8^{49} \equiv 1 \pmod{49}
\end{gathered}$$

Then,

$$6^{49} + 8^{49} \equiv 0 \pmod{49}$$

Therefore, we get:

$$49 | a_{49}$$

Note. We could restate the problem as :

Prove that there exists at least one positive integer n such that

$$n|a_n$$

Though the solution would remain same, this problem will be definitely a harder one than the previous.

88. Find all n such that

$$44\ldots\ldots44\ (n\text{times } 4)$$

is a perfect square.

Solution.

$$44\ldots\ldots44 = 4 \cdot 11\ldots\ldots11$$

If $n > 1$, then $44\ldots\ldots44$ ends in 11. From the theorem 4 of section 3.4.2, the number is

$$11 \equiv 3 \pmod 4$$

But every square is either 0 or 1 modulo 4. Thus, $n = 1$ and 4 is the only such number.

89. Find all positive integer solutions to the equation :

$$2^n - 1 = 3^m$$

Solution. First see that

$$2^n - 1 \equiv 0 \pmod 3$$

If n odd,

$$2^n - 1 \equiv (-1)^n - 1 \equiv -2 \pmod 3$$

That is, $2^n - 1$ is not divisible by 3. So, n must be even. Let $n = 2k$. We have

$$(2^k + 1)(2^k - 1) = 3^m$$

Since there is no other prime factors other than 3, we must have $2^k + 1$ and $2^k - 1$ both a power of 3. Say,

$$2^k - 1 = 3^a, 2^k + 1 = 3^b$$

where $a + b = m$.

$$3^b - 3^a = 2$$

If $a > 0$, we shall have that $3|2$. Therefore, $a = 0$ and then $b = 1$ leading to the solution $m = 1, n = 2$.

90. Prove that the sum of squares of three consecutive is not a square.

Solution. Let the integers be $n-1, n, n+1$. Then

$$(n-1)^2 + n^2 + (n+1)^2 = 2(n^2+1) + n^2 = 3n^2 + 2$$

This is congruent to 2 modulo 3. So, it is never a square.

91. Prove that if p and $8p^2+1$ both are primes then $8p^2-1$ is a prime too.

Solution. If $p = 2$, we have $8p^2 + 1 = 33$ not a prime. Now see when $p = 3$, we have

$$8p^2 + 1 = 73$$

and

$$8p^2 - 1 = 71$$

both prime. Consider $p > 3$. Then obviously

$$p^2 \equiv 1 \pmod 3$$

$$\Rightarrow 8p^2 + 1 \equiv 8 + 1 \equiv 0 \pmod 3$$

So, it won't be a prime. Thus, $p = 3$ is only such prime.

Question. What should make you convinced about taking (mod 3) ?

92. Find all n such that

$$n | 2^n - 1$$

Solution. Let p be the smallest prime factor of n.[1] Of-course n odd, so p odd too and

$$p | 2^n - 1$$

$$\Rightarrow 2^n \equiv 1 \pmod p$$

Moreover, from Fermat's theorem,

$$2^{p-1} \equiv 1 \pmod p$$

Thus from proposition 10,

$$2^{(p-1,n)} \equiv 1 \pmod p$$

[1]This idea is a very important tactic for solving a good number of problems, even at the IMO

The crucial argument: note that $p-1$ won't share any prime factor with $p-1$. If n shares a prime with $p-1$ that must be strictly less than p. But it would contradict the fact that p is the smallest prime factor of p. Then

$$(n, p-1) = 1$$

Conclusion :

$$2^1 \equiv 1 \pmod{p}$$

Clearly contradiction!

This means that n can't have any prime factor i.e. $n = 1$.

93. If[2]

$$x^3 + y^3 = z^3$$

then one of x, y, z is divisible by 7.

Solution. Remember

$$x^3 \equiv 0, \pm 1 \pmod{7}$$

If $x^3 \equiv 0 \pmod{7}$, we are done. Else let

$$x^3 \equiv \pm 1 \pmod{7}$$

Also, $y^3 \equiv \pm 1 \pmod{7}$ and $z^3 \equiv \pm 1 \pmod{7}$ If $x^3 \equiv 1$ and $y^3 \equiv 1$, then

$$\pm 1 \equiv z^3 \equiv 2$$

so it is a contradiction.

Similarly,

$$x^3, y^3 \not\equiv -1$$

Then one of

$$x^3 \equiv 1, y^3 \equiv -1$$

And then

$$x^3 + y^3 \equiv 0 \pmod{7}$$
$$\Rightarrow z^3 \equiv 0 \pmod{7}$$

Remark 8. Here the modulo taken everywhere is 7, so sometimes it is not stated.

94. Find all primes p such that $2^p + p^2$ is a prime.

[2]Don't be tempted by *Fermat's Last Theorem*, because it is to be proved if it holds.

Solution. If $p = 2$, it is even greater than 2. So, p must be odd.

If $p = 3$, $2^3 + 3^2 = 17$, a prime. If $p > 3$, we have

$$p^2 \equiv 1 \pmod 3$$

Moreover,

$$2^p \equiv (-1)^p \equiv -1 \pmod 3$$

Summing these yields

$$2^p + p^2 \equiv 0 \mod 3$$

Thus, it is not a prime.

Hence, $p = \boxed{3}$ is the only solution.

5.2 Problems Without Solutions

95. Prove the congruences in section 2.4.1 .

96. Prove the divisibility facts in section 2.4.2 .

97. Without Fermat's theorem, prove that

$$13|n^{13} - n$$

$$10|a^5 - a$$

for any $n, a \in \mathbb{N}$

98. Generalize the fact $1, 3, 6$. Find the condition, when a number is divisible by 2^k.

99. Find all integers a such that $a + 3$, $a - 1$ and $a + 4$ are primes.

Hint. Think mod3.

100. Prove that the product of n consecutive integers is divisible by $n!$.

Hint. Is there anything to do with binomial coefficient?

101. Find all positive integer solutions to the equation :

$$2^n + 1 = 3^m$$

102. Prove that the sum of squares of five consecutive integers is not again a square.

103. x, y, z are positive integers such that:

$$x^3 + y^3 = z^3$$

then $3|xyz$.

104. Find all solution to the diophantine equation :

$$3^x - 2^y = 7$$

105. Find another Carmichael number.

106. Find all primes p, q such that

$$pq|(5^p - 2^p)(5^q - 2^q)$$

107. Prove that,

$$77|36^{36} + 41^{41}$$

108. Does there exists a prime three distinct primes p, q, r such that,

$$p|q + r$$

$$q|r + p$$

$$r|p + q$$

109. Find all n such that $\varphi(n)$ is odd.

110. Find the last three digits of 7^{1999}