1. PRIMES

In the previous lecture you have learned about the fundamental theorem of arithmetic. In today’s lecture, we start by saying why there are infinitely many primes.

**Theorem 1** (Euclid’s theorem). There are infinitely many primes.

**Proof.** Suppose to the contrary that there are only finitely many primes, and they are

\[ p_1, p_2, \ldots, p_n. \]

Consider \( N := p_1p_2\cdots p_n + 1. \) Suppose \( p \) is a prime factor of \( N; \) notice that there is such a prime \( p \) as any integer more than 1 can be written as a product of primes. Since for any \( i \) the remainder of \( N \) divided by \( p_i \) is 1, \( p \neq p_i \) for any \( i. \) This contradicts our assumption that \( p_1, \ldots, p_n \) are all the primes. \( \square \)

The sequence of primes is very fascinating as they are both very structured and fairly random. Next I will present a conjecture which indicates in what sense primes are random.

**Definition 2** (Möbius function). Suppose \( n := p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}, \) \( p_i 's \) are distinct primes, and \( k_i 's \) are positive integers (so this is the prime factorization of \( n \)). We let

\[
\mu(n) = \begin{cases} 
1 & \text{if } n = 1, \\
0 & \text{if } \exists i, k_i \geq 2, \\
(-1)^r & \text{if } r \geq 1 \text{ and } \forall i, k_i = 1.
\end{cases}
\]

One can prove that

\[
\lim_{n \to \infty} \frac{\mu(1) + \mu(2) + \cdots + \mu(n)}{n} = 0,
\]
this means we can see a lot of cancellations. In fact the famous Riemann Hypothesis is equivalent to saying that for any \( \varepsilon > 0 \) we should have
\[
\lim_{n \to \infty} \frac{\mu(1) + \mu(2) + \cdots + \mu(n)}{n^{1+\varepsilon}} = 0;
\]
we say we have \( a(n) \) (almost) square-root cancellation. I encourage you to write a code and find out how small this fraction gets; doing so you see how hard it is to find the prime factorization of a given integer.

2. Valuations, divisors, and perfect squares

2.1. Definition and the basic property. By the fundamental theorem of arithmetic any integer \( n > 1 \) can be written as
\[
2^{v_2(n)}3^{v_3(n)}5^{v_5(n)} \cdots
\]
for a unique sequence of non-negative integers \( \{v_p\}_{p \in \mathcal{P}} \) where \( \mathcal{P} \) is the set of primes and we are using the convention that the product of infinitely many 1’s is 1. So to any positive integer \( n \) we can associate a sequence of non-negative integers \( \{v_p(n)\}_{p \in \mathcal{P}} \) with the following property:
\[
(1) \quad n = \prod_{p \in \mathcal{P}} p^{v_p(n)};
\]
equivalently
\[
p^{v_p(n)} \mid n \text{ and } p^{v_p(n)+1} \nmid n,
\]
which means \( p^{v_p(n)} \) is the largest power of \( p \) that divides \( n \). For instance
\[
v_2(10) = 1, v_3(10) = 0, v_5(10) = 1, v_p(10) = 0 \text{ for any prime } p > 5.
\]
The quantity \( v_p(n) \) is called the \( p \)-valuation of \( n \). Here is an important property of the \( p \)-valuation \( v_p : \mathbb{Z}^+ \to \mathbb{Z}^{\geq 0} \).

**Lemma 3.** For any positive integers \( m \) and \( n \), and any prime \( p \), we have
\[
v_p(mn) = v_p(m) + v_p(n).
\]

**Proof.** We have \( m = \prod_{p \in \mathcal{P}} p^{v_p(m)} \) and \( n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \). Hence
\[
mn = \prod_{p \in \mathcal{P}} p^{v_p(m)} \cdot \prod_{p \in \mathcal{P}} p^{v_p(n)} = \prod_{p \in \mathcal{P}} (p^{v_p(m)} \cdot p^{v_p(n)}) = \prod_{p \in \mathcal{P}} p^{v_p(m)+v_p(n)},
\]
and so by the uniqueness of the prime factorization of \( mn \), we have
\[
v_p(mn) = v_p(m) + v_p(n);
\]
and claim follows.  

2.2. **Valuations and divisors.** Based on Lemma 3 we get the following criterion of divisibility:

**Lemma 4.** Suppose $d$ and $n$ are two positive integers. Then 

$$d|n \iff \forall p \in \mathcal{P}, v_p(d) \leq v_p(n).$$

(This type of result that certain properties from primes imply a similar result for integers is called *local-to-global*. This is a baby version of a local-to-global result.)

**Proof.** $(\Rightarrow)$ Since $d|n$ and $d, k$ are positive, we have that $n = dk$ for some positive integer $k$. Hence $v_p(n) = v_p(dk) = v_p(d) + v_p(k) \geq v_p(d)$; and claim follows.

$(\Leftarrow)$ Let $k := \prod_{p \in \mathcal{P}} p^{v_p(n) - v_p(d)}$. Since for any $p \in \mathcal{P}$ we have $v_p(n) \geq v_p(d)$ and $v_p(n) = v_p(d) = 0$ when $p$ is large enough, we deduce that $k$ is a positive integer. Then

$$dk = \prod_{p \in \mathcal{P}} p^{v_p(d)} \cdot \prod_{p \in \mathcal{P}} p^{v_p(n) - v_p(d)} = \prod_{p \in \mathcal{P}} p^{v_p(d) + (v_p(n) - v_p(d))} = \prod_{p \in \mathcal{P}} p^{v_p(n)} = n;$$

and so $d|n$.  

We can use Lemma 4 to give formula for the number of positive divisors of a positive integer.

**Lemma 5.** Let $d(n)$ be the number positive divisors of a positive integer $n$. Then 

$$d(n) = \prod_{p \in \mathcal{P}} (v_p(n) + 1).$$

**Proof.** By Lemma 4, $d|n$ if and only if $v_p(d) \leq v_p(n)$ for any $p \in \mathcal{P}$. So $v_p(d)$ is in the set $\{0, 1, \ldots, v_p(n)\}$, which means there are $v_p(n) + 1$ possibilities for $v_p(d)$. Since $v_p(d)$’s can be chosen independently (that means $v_2(d)$ can be any element in $\{1, \ldots, v_2(n)\}$, $v_3(d)$ can be any element in $\{1, \ldots, v_3(n)\}$, etc), we see that there are exactly $\prod_{p \in \mathcal{P}} (v_p(n) + 1)$ many possibilities for the sequence $\{v_p(d)\}_{p \in \mathcal{P}}$. Since this sequence uniquely determines the positive integer $d$, we get that $n$ has exactly $\prod_{p \in \mathcal{P}} (v_p(n) + 1)$ many positive divisors.
For instance $360 = 2^3 \times 3^2 \times 5$, implies that $v_2(360) = 3$, $v_3(360) = 2$, $v_5(360) = 1$, and $v_p(360) = 0$ for any prime $p > 5$. Hence the number of positive divisors of 360 is
\[ d(360) = (3 + 1) \cdot (2 + 1) \cdot (1 + 1) = 24. \]

2.3. Valuations and perfect squares. Notice that $v_p(n^2) = 2v_p(n)$ is even for any positive integer $n$ and prime $p$. Hence $v_p(n^2) + 1$ is odd, which implies that
\[ d(n^2) = \prod_{p \in \mathcal{P}} (v_p(n^2) + 1) = \prod_{p \in \mathcal{P}} (2v_p(n) + 1) \]
is odd. As you will show in your homework assignment the converse of this statement also holds:

\emph{m is a perfect square if and only if the number of its positive divisors is odd.}

(There is an alternative approach to show the above claim using the fact that a positive divisor $d$ of $n$ can be paired with $n/d$, unless $d = n/d$ for some divisor $d$. If $d = n/d$, then $n = d^2$ is a perfect square.)

Next we show that $\sqrt{2}$ is not a rational number.

\textbf{Proposition 6.} $\sqrt{2}$ is not a rational number.

\textit{Proof.} Suppose to the contrary that there are positive integers $m$ and $n$ such that $\sqrt{2} = \frac{m}{n}$. Then $2n^2 = m^2$; this implies that
\[ v_2(2n^2) = v_2(m^2); \quad \text{and so} \quad 2v_2(n) + 1 = 2v_2(m), \]
which is a contradiction as the left hand side is odd and the right hand side is even. \hfill \square

This argument is quite strong and general; based on this argument you can easily show that $\sqrt[n]{k}$ is not a rational number if $k \nmid v_p(n)$ for some prime $p$.

3. Congruence arithmetic

3.1. Definition and equivalence relation properties. We say \emph{a is congruent to b modulo n} and write
\[ a \equiv b \pmod{n} \]
if $n|a - b$. For instance $12 \equiv 2 \pmod{5}$ and $13 \equiv 5 \pmod{4}$. It is like labeling $n$ points on a circle starting by 0 and going clockwise; then
\[ 0, n, 2n, \ldots \]
label the same point. Similarly

$$1, n + 1, 2n + 1, \ldots$$

label the same point. In general, $a$ and $b$ label the same point precisely when $a$ is congruent to $b$ modulo $n$.

One can interpret clock as representing the hours modulo 12. So modulo $n$ numbers can be interpreted as the clocks in a planet that has $n$ hours in a day. In a sense we are treating the one O’clock the same in all the days. In technical terms $a \equiv b \pmod{n}$ is an equivalence relation. This means the following properties:

**Lemma 7** (Equivalence relation). The following properties hold:

1. $a \equiv a \pmod{n}$.
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
3. $\begin{cases} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{cases} \Rightarrow a \equiv c \pmod{n}$.

**Proof.** Notice that any non-zero integer divides 0; and so $n|a - a$, which implies that $a \equiv a \pmod{n}$.

The second part follows from the fact that if $n$ divides $x$, then it divides $-x$:

$$a \equiv b \pmod{n} \implies n|a - b \implies n|b - a \implies b \equiv a \pmod{n}.$$  

For the third part we use the fact that if $n$ divides $x$ and $y$, then it divides $x + y$.

$$\begin{cases} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{cases} \implies n|a - b \implies n|b - c \implies n|(a - b) + (b - c) \implies n|a - c \implies a \equiv c \pmod{n}.$$  

\[\square\]

### 3.2. Doing arithmetic with numbers congruent modulo $n$.

The following result is the main reason why considering integers congruent modulo $n$ is extremely useful.

**Lemma 8.** Suppose $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$; then

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n} \text{ and } a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}.$$
Proof. The first claim follows from the fact that if \( n \) divides \( x \) and \( y \), then \( n \) divides \( x + y \):

\[
\begin{align*}
  a_1 &\equiv a_2 \pmod n \quad \implies \quad n|a_1 - a_2 \quad \implies \quad n|(a_1 - a_2) + (b_1 - b_2) \\
  b_1 &\equiv b_2 \pmod n \quad \implies \quad n|b_1 - b_2 \quad \implies \quad n|(a_1 + b_1) - (a_2 + b_2) \\
  &\implies \quad a_1 + b_1 \equiv a_2 + b_2 \pmod n.
\end{align*}
\]

The second part follows from the fact that if \( n \) divides \( x \) and \( y \), then it divides any integer linear combination \( rx + sy \) of \( x \) and \( y \):

\[
\begin{align*}
  a_1 &\equiv a_2 \pmod n \quad \implies \quad n|a_1 - a_2 \\
  b_1 &\equiv b_2 \pmod n \quad \implies \quad n|b_1 - b_2 \\
  &\implies \quad n|b_1(a_1 - a_2) + a_2(b_1 - b_2) \\
  &\implies \quad n|(b_1 \cdot a_1 - b_1 \cdot a_2) + (a_2 \cdot b_1 - a_2 \cdot b_2) \\
  &\implies \quad n|a_1 \cdot b_1 - a_2 \cdot b_2 \\
  &\implies \quad a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod n.
\end{align*}
\]

\[\square\]

3.3. Congruence arithmetic and finding remainders. Here we see an example of how working with numbers congruent modulo \( n \) can help us find the remainder of a division by \( n \).

Example 9. Find the remainder of 10020192018 divided by 9.

Solution. We notice that \( 10 \equiv 1 \pmod 9 \); and so for any positive integer \( m \) we have

\[
10^m = 10 \times \cdots \times 10 \equiv 1 \times \cdots \times 1 = 1.
\]

Hence any number is congruent to the sum of its digits modulo 9:

\[
10020192018 \equiv 10^{10} + 2 \times 10^7 + 1 \times 10^5 + 9 \times 10^4 + 2 \times 10^3 + 1 \times 10 + 8 \\
\equiv 1 + 2 + 1 + 9 + 2 + 1 + 8 \\
\equiv 6.
\]

Suppose \( r \) is the remainder of this division. Then 10020192018 − \( r \) is a multiple of 9, which means

\[
10020192018 \equiv r \pmod 9.
\]
By the above computation, we deduce that

\[ r \equiv 6 \pmod{9}. \]

Since \( r \) is the remainder of this division, we have \( 0 \leq r < 9 \). Hence \(-6 \leq r - 6 < 3\) and \( 9 \mid r - 6 \); the only multiple of 9 in this range is 0. Hence \( r - 6 = 0 \), which means the remainder \( r \) of this division is 6.