Math 342. Notes for Lecture 8. January 30, 2018

Modular arithmetic

Recall that $a_1 \equiv a_2 \pmod{n}$ if $a_1$ and $a_2$ have the same remainder when divided by $n$. Equivalently, $a_1 \equiv a_2 \pmod{n}$ if $a_2 - a_1$ is divisible by $n$.

For example, $99 \equiv 6 \pmod{31}$ and $6 \equiv -2 \pmod{4}$.

We showed that if $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$, $a_1 - b_1 \equiv a_2 - b_2 \pmod{n}$, and $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.

Example: $49 \cdot 48 \equiv 4 \cdot 3 \equiv 12 \equiv 2 \pmod{5}$.

Another example: Using $521 \equiv 1 \pmod{5}$, $10234 \equiv 4 \equiv -1 \pmod{5}$, and $723 \equiv 3 \equiv -2 \pmod{5}$, we obtain

$$521^{1000} + 10234^{500} \cdot 723^{4} \equiv 1^{1000} + (-1)^{500} \cdot (-2)^{4} \equiv 1 + 1 \cdot 16 \equiv 1 \pmod{5}.$$  

Remark: If $d \equiv e \pmod{n}$, we cannot conclude that $a^d \equiv a^e \pmod{n}$. For example, $1 \equiv 4 \pmod{3}$ but

$$2^1 \not\equiv 2^4 \pmod{3}.$$  

Indeed, $2^1 \equiv 2 \pmod{3}$ and $2^4 \equiv 16 \equiv 1 \pmod{5}$.

The Euclidean algorithm

Defn: Let $a$ and $b$ be positive integers. The greatest common divisor of $a$ and $b$ (written gcd$(a,b)$, or sometimes $(a,b)$) is the largest integer which is a divisor of $a$ and $b$.

Example: gcd$(30, 45) = 15$, gcd$(30, 49) = 1$.

The Euclidean Algorithm is an efficient method for finding the gcd.
Lemma: $\gcd(a, b) = \gcd(a - qb, b)$ for any integer $n$.

Proof: The common divisors of $a$ and $b$ are the same as the common divisors of $a + nb$ and $b$. (Check!) Thus the greatest common divisor is the same. \hfill \Box

The Euclidean algorithm applies the above lemma recursively. We arrange $a, b$ so that $a \geq b$ and $b > 0$. Divide $a$ by $b$ with remainder $r$.

Each subsequent step consists of replacing $(a, b)$ by $(b, r)$.

This does not change the gcd, and both $a$ and $b$ become smaller. Continue as long as the second number remains positive. Stop when $r = 0$. At this point $\gcd(b, r) = \gcd(b, 0) = b$, and we are done.

Example 1: $a = 154, b = 35$. Euclidean algorithm:

$\begin{align*}
154 &= 4 \cdot 35 + 14 \\
35 &= 2 \cdot 14 + 7 \\
14 &= 2 \cdot 7 + 0.
\end{align*}$

Conclusion: $\gcd(154, 35) = 7$.

Example 2: $a = 553, b = 327$. Euclidean algorithm:

$\begin{align*}
553 &= 1 \cdot 327 + 226 \\
327 &= 1 \cdot 226 + 101 \\
226 &= 2 \cdot 101 + 24 \\
101 &= 4 \cdot 24 + 5 \\
24 &= 4 \cdot 5 + 4 \\
5 &= 1 \cdot 4 + 1 \\
4 &= 1 \cdot 4 + 0.
\end{align*}$

Conclusion: $\gcd(553, 327) = 1$.

Bezout’s equation
We will now use the Euclidean algorithm to “quickly” find an integer solution to the equation $ax + by = \gcd(a, b)$ for any given pair of integers $a \geq b > 0$.

In particular, we will see that this equation always has a solution.

Set

$$r_{-1} = b, \quad r_0 = a$$

$$r_{-1} = r_0 q_0 + r_1, \quad 0 \leq r_1 < r_0$$

$$r_0 = r_1 q_1 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3, \quad 0 \leq r_3 < r_2$$

$$\ldots$$

$$r_{i-1} = r_i q_i + r_{i+1}, \quad 0 \leq r_{i+1} < r_i$$

$$\ldots$$

$$r_{j-2} = r_{j-1} q_{j-1} + r_j, \quad 0 \leq r_j < r_{j-1}$$

$$r_{j-1} = r_j q_j$$

Here $\gcd(a, b) = r_j$. First we express it as a linear combination of $r_{j-1}$ and $r_{j-2}$ with integer coefficients, using the second to last equation,

$$\gcd(a, b) = r_j = r_{j-2} - q_{j-1} r_{j-1}.$$

Now we use the next equation, $r_{j-3} = q_{j-2} r_{j-2} + r_{j-1}$ to eliminate $r_{j-1}$ and express $\gcd(a, b)$ as a linear combination of $r_{j-3}$ and $r_{j-2}$. Continue until $\gcd(a, b)$ is expressed as an integer linear combination of $r_{-1} = a$ and $r_0 = b$.

Back to Example 1: Solve $154x + 35y = 7$. Euclidean algorithm:

$$154 = 4 \cdot 35 + 14$$

$$35 = 2 \cdot 14 + 7$$

$$14 = 2 \cdot 7 + 0.$$
Back substitution:

\[ 7 = 35 - 2 \cdot 14 = 35 - 2 \cdot (154 - 4 \cdot 35) = 35 - 2 \cdot 154 + 8 \cdot 35 = (-2) \cdot 154 + 9 \cdot 35. \]

Integer solution to \( 154x + 35y = 7 \): \( x = -2, \ y = 9 \).

Back to Example 2: \( a = 553, b = 327 \). Euclidean algorithm:

\[
egin{align*}
553 &= 1 \cdot 327 + 226 \\
327 &= 1 \cdot 226 + 101 \\
226 &= 2 \cdot 101 + 24 \\
101 &= 4 \cdot 24 + 5 \\
24 &= 4 \cdot 5 + 4 \\
5 &= 1 \cdot 4 + 1 \\
4 &= 1 \cdot 4 + 0.
\end{align*}
\]

Solve \( 553x + 327y = 1 \) by back substitution:

\[
\begin{align*}
1 &= (1 \cdot 5) + (-1 \cdot 4) = (-1 \cdot 24) + (5 \cdot 5) = (5 \cdot 101) + (-21 \cdot 24) \\
&= (-21 \cdot 226) + (47 \cdot 101) = (47 \cdot 327) + (-68 \cdot 226) = (-68 \cdot 553) + (115 \cdot 327)
\end{align*}
\]

Solution: \( x = -68, \ y = 115 \).

**Bezout’s Theorem:** Let \( a, b \) and \( c \) be integers, \( (a, b) \neq (0, 0) \). The equation \( ax + by = c \) has an integer solution \( x, y \) if and only if \( c \) is divisible by \( \gcd(a, b) \).

**Proof.** Denote \( \gcd(a, b) \) by \( d \). If \( c \) is divisible by \( d \), then, as we just saw, we can find integers \( x_0 \) and \( y_0 \) such that \( ax_0 + by_0 = d \). Now \( x = \frac{c}{d}x_0 \) and \( y = \frac{c}{d}y_0 \) are integer solutions of \( ax + by = c \) (Check!).

Conversely, since \( d \) divides both \( a \) and \( b \), it divides \( ax + by \), for any integers \( x \) and \( y \). Thus if \( c \) is not divisible by \( d \), then \( ax + by \) can never be equal to \( c \), for any integers \( x \) and \( y \).  \( \square \)
Multiplicative inverses mod $n$

To find the multiplicative inverse of $a$ in $\mathbb{Z}_n$ means to find an integer $x$ such that $ax \equiv 1 \pmod{n}$. This means finding integers $x$ and $y$ such that $ax - ny = 1$.

Theorem: (1) $a$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$.

(2) $\mathbb{Z}_n$ is a field if and only if $n$ is a prime.

Proof: (1) If $\gcd(a, n) = 1$, we just saw that $ax - ny = 1$ has an integer solution. Conversely, if $\gcd(a, n) = d > 1$, then any integer linear combination $ax - ny$ will be divisible by $d$. Hence, in this case $ax - ny$ can never be 1.

(2) If $n$ is a prime, then for every $a = 1, \ldots, p - 1$, $\gcd(a, n) = 1$. Hence, every non-zero $a$ in $\mathbb{Z}_n$ has a multiplicative inverse. Since we already know that $\mathbb{Z}_n$ is a ring for any $n$, this shows that it is a field when $n$ is a prime.

On the other hand, suppose $n$ is not a prime, say $n = km$, where $k, m > 1$ are integers. Then $\gcd(k, n) = k > 1$. Hence, $k$ is not invertible in $\mathbb{Z}_n$. \qed