Notes

September 3, 2014

1.1 #11

if $a > 0$ then $(ab, ac) = a(b, c)$
assume $a, b, c \in \mathbb{Z}, a > 0$

$$\begin{aligned} d &= (ab, ac) \\ d &= mab + mac \text{ theorem 1.1.6} \\ &= a(mb + nc) \text{ this is a linear combination of gcd for } a, b \\ mb + nc &\in \gcd(b, c)\mathbb{Z} \\ d &= ad_1 \end{aligned}$$

now prove that $d|ad_1$.

$$\begin{aligned} d_1 &= m'b + n'c \text{ for some } m', n' \in \mathbb{Z} \\ ad_1 &= m'ab + n'ac \\ d &= (ab, ac) \to d|m'ab + n'ac \to d|ad_1 \end{aligned}$$

$3x + 7$ divisible by 11 (problem 22)

$x = 11 + 5k, k \in \mathbb{Z}$, note there are infinitely many solutions, and the difference between any two solutions is 11

if $x = 5 + 11k$ for $k \in \mathbb{Z}$ then $3x + 7 = 3(5 + 11k) + 7$

assume $3x + 7$ is divisible by 11. $11q + r = x, 0 \leq r < 10$ then $3x + 7 = 3(11q + r) + 7 = 33q + 3r + 7$ so $3r + 7$ is divisible by 11. we know that $0 \leq r < 11$ so $7 \leq 3r + 7 \leq 37$, $3r + 7 \in \{11, 22, 33\} \to r = 5$

fundamental theorem of arithmetic

any integer $a > 1$ can be factored uniquely as a product of prime numbers. $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n} ...$ with $p_1 < p_2 < ... < p_n$ and $\alpha_1, \alpha_2, ...\alpha_n$ positive integers

least common multiple

given $a, b \in \mathbb{Z}^+$, we say that the positive integer m is the lcm of a and b if

1. $a|m$ and $b|m$
2. if $a|c$ and $b|c$ then $m|c$

fact

$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$
$b = p_1^{\beta_1} p_2^{\beta_2} ... p_n^{\beta_n}$
$p_1 < p_2 < ... < p_n, \alpha_i, \beta_i \geq 0$
then $(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} ... p_n^{\min\{\alpha_n,\beta_n\}}$
then $[a, b] = p_1^{\max\{\alpha_1,\beta_1\}} ... p_n^{\max\{\alpha_n,\beta_n\}}$

example

$$
\begin{aligned}
6 &= 2^1 3^1 5^0 \\
15 &= 2^0 3^1 5^1 \\
(6, 15) &= 2^0 3^1 5^0 = 3 \\
[6, 15] &= 2^1 3^1 5^1 = 30
\end{aligned}
$$

observe

$(a, b)[a, b] = ab$
least common multiple of a, b is ab

congruences

definition

given $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}, n > 0$ we say that $a \equiv b \mod n$ if a and b give the same remainder when divided by n
exercise from last time showed $a \equiv b \mod n \Leftrightarrow n|(a - b)$

properties

1. $$
\begin{aligned}
a &\equiv b \mod n \\
c &\equiv d \mod n
\end{aligned}
$$

   implies

   $$a \pm c \equiv b \pm d \mod n$$

   and

   $$ac \equiv bd \mod n$$

   #### proof

   we prove that $ac \equiv bd \mod n$

   we know that $n|(a - b)$ and $n|(c - d)$. write that $a - b = n\alpha, \alpha \in \mathbb{Z}$ and $c - a = n\beta, \beta \in \mathbb{Z}$ then $ac - bd = (b + n\alpha)(d + m\beta) - bd =$multiple of $n\square$

2. $a \in \mathbb{Z}, n > 1, n \in \mathbb{Z}$ then there exist $b \in \mathbb{Z}$ such that $ab \equiv 1 \mod n$ if and only if $(a, n) = 1$

   note $3x + 7$ divisible by 11 is like saying $3x \equiv -7 \equiv 4 \mod 11$. $12x \equiv -28 \mod 11$

proof

$\Rightarrow$

assume $ab \equiv 1 \mod n$ for some $b \in \mathbb{Z}$. Then $ab - 1 = n\alpha$ for some $\alpha \in \mathbb{Z}$ and $ab + n\alpha = 1 \rightarrow d = (a, b)$ so $d|1 \rightarrow d = 1$

$\Leftarrow$

assume $(a, n) = 1$. there exist $\alpha, \beta \in \mathbb{Z}$ such that $a\alpha + n\beta = 1$ and then $a\alpha \equiv 1 \mod n$