Probability

- *Random variable* (r.v.): variable that takes on (discrete) values with certain probabilities

- *Probability distribution*: for an r.v. specifies the probabilities with which the variable takes on each possible value
  - Each probability must be between 0 and 1
  - The probabilities must sum to 1

- *Event*: a particular occurrence in some experiment
  - $\Pr[E]$: probability of event E

- *Conditional probability*: probability that one event occurs, given that some other even occurred
  - $\Pr[A \mid B] = \Pr[A \text{ and } B]/\Pr[B]$

- Two r.v.'s X, Y are *independent* if for all x, y: $\Pr[X = x \mid Y = y] = \Pr[X = x]$

- *Law of total probability*: say $E_1, \ldots, E_n$ are a partition of all possibilities. Then for any A: $\Pr[A] = \sum_i \Pr[A \text{ and } E_i] = \sum_i \Pr[A \mid E_i] \cdot \Pr[E_i]$

- *Bayes's theorem*

$$\Pr[A \mid B] = \Pr[B \mid A] \cdot \Pr[A]/\Pr[B]$$

Number Theory

费马小定理 (Fermat's Law)

设p为素数，a是任意整数，则 $a^p \equiv a \pmod p$

若a不是p的倍数，则 $a^{p-1} \equiv 1 \pmod p$

证明：

Lemma 1: $a,b,c \in \mathbb{Z}$, $m \in \mathbb{Z}^*$ 且 $\gcd(m,c)=1$. 则当 $ac \equiv bc \pmod m$ 时，$a \equiv b \pmod m$

$\because ac \equiv bc \pmod m$ $\quad \therefore (a-b)c \equiv 0 \pmod m$

$\because \gcd(m,c)=1$ $\quad \therefore a-b \equiv 0 \pmod m \Rightarrow a \equiv b \pmod m$

Lemma 2:

贝祖定理 (Bezout's Law):

设a,b为不全为0的整数，则存在整数x,y，使得 $ax+by=\gcd(a,b)$.

证明：①若a,b其一为0，设b=0，则 $\gcd(a,b)=a$ 满足

②若 $a,b\neq 0$. 设 $a,b>0$ 且 $a\geq b$，$\gcd(a,b)=d$. 则有

$ax+by=d \Rightarrow a'x+b'y=1$，其中 $\gcd(a',b')=1$.

(贝祖定理的一个引理：若 $\gcd(a,b)=1$，则 $\exists x,y\in\mathbb{Z}$，$ax+by=1$)

由辗转相除法可知：$\gcd(a,b)=\gcd(b,r_1)=\gcd(r_1,r_2)=\dots=\gcd(r_{n-1},r_n)$
$=\gcd(r_n,0)=r_n$

也即：
$$
\begin{aligned}
a &= q_1 b + r_1\\
b &= q_2 r_1 + r_2\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} + r_n\\
r_{n-1} &= q_{n+1} r_n
\end{aligned}
$$

假设在 r_{n-1} 与 r_{n-2} 互质时退出，即

$r_{n-2}=x_n r_{n-1}+1 \Rightarrow 1=r_{n-2}-x_n r_{n-1}$

将 $r_{n-1}=r_{n-3}-x_{n-1}r_{n-2}$ 代回上式，有

$1=(1+x_n x_{n-1})r_{n-2}-x_n r_{n-3}$

不断回代可得x,y的值从而 $ax+by=1$.

We can use extended Euclidean algorithm to find Bezout's identity.

Example: Express $\gcd(252,198)=18$ as a linear combination of 252 an
198.

Solution: To show that $\gcd(252,198)=18$, the Euclidean algorithm us
these divisions:

$$
\begin{aligned}
252 &= 1\cdot 198 + 54\\
198 &= 3\cdot 54 + 36\\
54 &= 1\cdot 36 + 18\\
36 &= 2\cdot 18.
\end{aligned}
$$

Substituting the above expressions:

$$18 = 54 - 1\cdot 36 = 54 - 1\cdot(198 - 3\cdot 54) = 4\cdot 54 - 1\cdot 198.$$

$$18 = 4\cdot(252 - 1\cdot 198) - 1\cdot 198 = 4\cdot 252 - 5\cdot 198.$$

逆元:

对正整数 a, m，若有 $ax \equiv 1 \pmod m$，则 x 的最小正整数解为 a 模 m 的逆元。

$\gcd(a,m)=1,\ m>1 \iff ax \equiv 1 \pmod m$ 有解

逆元求法：①费马小定理：$a \cdot a^{p-2} \equiv 1 \pmod p \Rightarrow a^{p-2} \bmod p$ 为 a 的逆元

②扩展欧几里得算法(贝祖定理利用)：求解 $ax+by=\gcd(a,b)$ 的 x, y.

Using extended Euclidean algorithm:

Example: Find an inverse of 101 modulo 4620. That is, find $\bar{a}$ such that $\bar{a} \cdot 101 \equiv 1 \pmod{4620}$.

$$
\begin{aligned}
4620 &= 45 \cdot 101 + 75 \\
101 &= 1 \cdot 75 + 26 \\
75 &= 2 \cdot 26 + 23 \\
26 &= 1 \cdot 23 + 3 \\
23 &= 7 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
1 &= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\
1 &= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \\
1 &= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75 \\
1 &= 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75 \\
&= 26 \cdot 101 - 35 \cdot 75 \\
1 &= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) \\
&= -35 \cdot 4620 + 1601 \cdot 101
\end{aligned}
$$

That $-35 \cdot 4620 + 1601 \cdot 101 = 1$ tells us that -35 and 1601 are Bezout coefficients of 4620 and 101. We have

$$1 \bmod 4620 = 1601 \cdot 101 \bmod 4620.$$

Thus, 1601 is an inverse of 101 modulo 4620.

欧拉函数:

$\varphi(n)$，表示小于等于 n 和 n 互质的数的个数。

当 n 为质数时，$\varphi(n)=n-1$

若 $\gcd(a,b)=1$，则 $\varphi(a \times b)=\varphi(a) \times \varphi(b)$

当 n 是奇数时，$\varphi(2n)=\varphi(n)$

欧拉定理：若 $\gcd(a,m)=1$，则 $a^{\varphi(m)} \equiv 1 \pmod m$

中国剩余定理:

同余方程组
$$
\begin{cases}
x \equiv a_1 \pmod{m_1} \\
x \equiv a_2 \pmod{m_2} \\
\quad \vdots \\
x \equiv a_n \pmod{m_n}
\end{cases}
$$
中 m_i 两两互质

有唯一解 $x \bmod m$ $(m=m_1 m_2 \cdots m_n)$

步骤：①计算模数之积：$m=\prod_i m_i$

②对第 i 个方程，计算

i) $M_i = \frac{m}{m_i}$

ii) M_i 模 m_i 下的逆元 M_i^{-1}

iii) $C_i = M_i M_i^{-1}$

③解为 $x = \sum_{i=1}^{k} a_i C_i \pmod m$

$$
\begin{aligned}
x &\equiv 2 \pmod 3 \\
x &\equiv 3 \pmod 5 \\
x &\equiv 2 \pmod 7
\end{aligned}
$$

1. Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, and $M_3 = m/7 = 15$.
2. Compute the inverse of M_k modulo m_k:
   - $35 \cdot 2 \equiv 1 \pmod 3$ $y_1 = 2$
   - $21 \equiv 1 \pmod 5$ $y_2 = 1$
   - $15 \equiv 1 \pmod 7$ $y_3 = 1$
3. Compute a solution x:
   $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23 \pmod{105}$
4. The solutions are all integers x that satisfy $x \equiv 23 \pmod{105}$.

回代法:

(1) $x \equiv 1 \pmod 5$
(2) $x \equiv 2 \pmod 6$
(3) $x \equiv 3 \pmod 7$

According to (1), $x = 5t + 1$, where t is an integer.

Substituting this expression into (2), we have $5t + 1 \equiv 2 \pmod 6$, which means that $t \equiv 5 \pmod 6$. Thus, $t = 6u + 5$, where u is an integer.

Substituting $x = 5t + 1$ and $t = 6u + 5$ into (3), we have $30u + 26 \equiv 3 \pmod 7$, which implies that $u \equiv 6 \pmod 7$. Thus, $u = 7v + 6$, where v is an integer.

Thus, we must have $x = 210v + 206$. Translating this back into a congruence,

$$x \equiv 206 \pmod{210}.$$