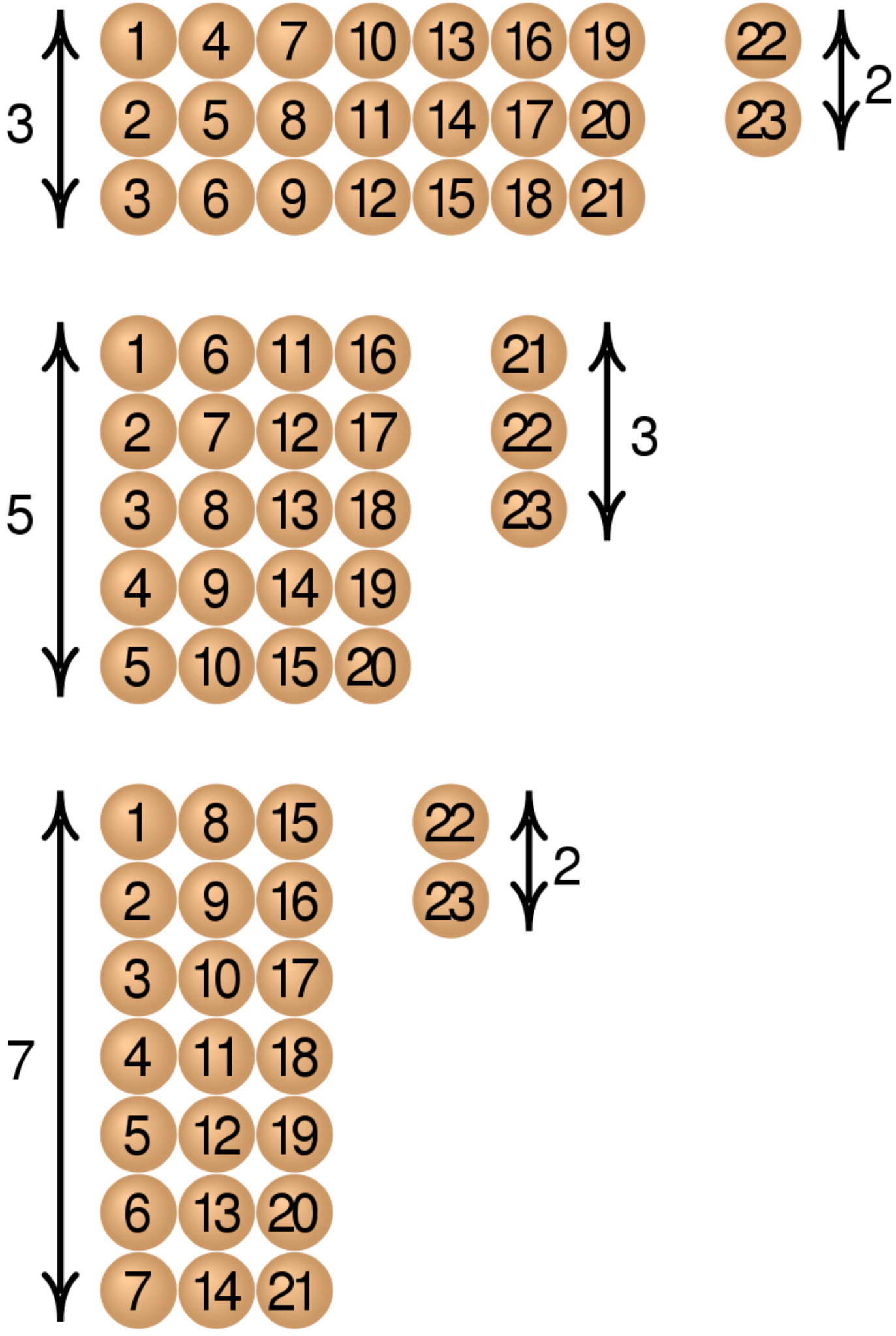
中国剩余定理简介 (CRT)：从入门到放弃

中国剩余定理（CRT）在公钥密码学中非常重要，是优化计算性能的一种常用技术。本次梳理一下CRT相关的知识。

0. 从入门


3
1 4 7 10 13 16 19
2 5 8 11 14 17 20
3 6 9 12 15 18 21
22 23
2
5
1 6 11 16
2 7 12 17
3 8 13 18
4 9 14 19
5 10 15 20
21 22 23
3
7
1 8 15
2 9 16
3 10 17
4 11 18
5 12 19
6 13 20
7 14 21
22 23
2

CRT最早是被孙子提出，用来进行兵力统计。他发现，如果士兵：

1. 3人一列，则剩余2人；
2. 5人一列，则剩余3人；
3. 7人一列，则剩余2人；

那么士兵的总人数应该是 23 人（人数$< 3 \times 5 \times 7$）。

推广一下，对于给定的 x 和 互素的 p_1, p_2, p_3，我们有

$$
\begin{aligned}
r_1 &= x \pmod{p_1}, \\
r_2 &= x \pmod{p_2}, \\
r_3 &= x \pmod{p_3}
\end{aligned}
$$

那么，我们在 $[0, p_1p_2p_3)$之内可以确定唯一的 x 满足上述要求。

1. 到放弃

1.1 定义

理论上，CRT描述了两个群之间的同构（isomorphisms，$\mathbb{G} \backsimeq \mathbb{H}$）：对于给定的$x \in \mathbb{G}$，我们可以找到其在群 $\mathbb{H}$ 中的对应元素。该映射是一一对应的，并且对于$\mathbb{G}$中的操作，在$\mathbb{H}$都可以进行对应计算。而进行这种映射的主要原因则是有些计算在$\mathbb{G}$复杂度很高，却能在$\mathbb{H}$中高效计算。
接下来以两个模数 $N = pq$其中$p, q > 1$且互素为例 (Case of two moduli)，梳理CRT的一些重要知识点

定义：令 $N = pq$，其中$p, q > 1$且互素，那么 $\mathbb{Z}_N \backsimeq \mathbb{Z}_p \times \mathbb{Z}_q$。进一步，定义映射 f：

$$
f(x) \stackrel{def}{=} ([x \pmod{p}], [x \pmod{q}]),
$$

其中 $x \in \mathbb{Z}_N$。

另外一种常见的表述则是 $p|x - r_1, q|x - r_2$，其中$0 \leq r_1 < p$，$0 \leq r_2 < q$。其实，此处的r_1和 r_2就是模约减对应的余数。

1.2 运算

CRT支持加法、乘法和指数计算。例如对于加法，有

$$
\begin{aligned}
f(a +_N b) &= ([a +_N b \pmod p], [a +_N b \pmod q]) \\
&= ([a + b \pmod p], [a + b \pmod q]) \\
&= ([a \pmod p], [a \pmod q]) \boxplus ([b \pmod p], [b \pmod q]) = f(a) \boxplus f(b)
\end{aligned}
$$

其中 $+_N$表示在$\mathbb{Z}_N$中的加法，$\boxplus$ 表示 $\mathbb{Z}_p \times \mathbb{Z}_q$下的加法。
一般的，利用CRT计算$g_1 \circ g_2$（$g_1, g_2 \in \mathbb{G}$）的步骤如下：

1. 计算映射 $h_1 = f(g_1), h_2 = f(g_2)$，；
2. 在 $\mathbb{H}$ 中计算 $h = h_1 \circ_{\mathbb{H}} h_2$；
3. 计算 $g = f^{-1}(h)$。

1.3 f^{-1}

对于 $f(x) = (x_p, x_q)$，我们有

$$
(x_p, x_q) = x_p \cdot (1, 0) + x_q \cdot (0, 1)
$$

因此，如果能找到 $1_p, 1_q \in \mathbb{Z}_N$ 满足 $f(1_p) = (1, 0), f(1_q) = (0, 1)$，那么则有

$$
f^{-1}(x_p, x_q) = [x_p \cdot 1_p + x_q \cdot 1_q \pmod N]
$$

而由于 $gcd(p, q) = 1$，必然存在 X, Y 满足

$$
Xp + Yq = 1
$$

由于 $Yq \pmod q = 0$ 且 $Yq = 1 - Xp = 1 \pmod p$，所以 $[Yq \pmod N] = 1_p$。同理 $[Xp \pmod N] = 1_q$。故，求 $f^{-1}(x_p, x_q)$的算法如下：

1. 计算 X, Y 得到 $Xp + Yq = 1$；
2. 令 $1_p = [Yq \pmod N]$，$1_q = [Xp \pmod N]$；
3. 计算 $[x_p \cdot 1_p + x_q \cdot 1_q \pmod N]$。

上述性质都可以拓展到多个模数 (General Case)，具体可以参考链接

另一个比较重要的点则是x的存在性和唯一性。该方面的证明可以参考柯俊明整理的资料。