Montgomery 乘算法

证明. 我们有 $T+Um\equiv T(\bmod m)$,因此,$(T+Um)R^{-1}\equiv TR^{-1}(\bmod m)$。
当$(T+Um)/R$为整数,$(T+Um)/R\equiv(T+Um)R^{-1}\equiv TR^{-1}(\bmod m)$,
也就是,$(T+Um)/R$ 是对 $TR^{-1}(\bmod m)$的估计。
由于 $U\equiv Tm'(\bmod R)$和 $m'\equiv -m^{-1}(\bmod R)$,我们可以假定
$U=Tm'+kR$ 和 $mm'=-1+lR$,这里k和 l是整数。因此,
$(T+Um)/R=(T+(Tm'+kR)m)/R=(T+T(-1+lR)+kRm)/R=$
$Tl+km$。

Barrett 约减方法

证明.目标：$r = x(\bmod m)$，$x = qm + r, 0 \le r < m$。

注意$q = \left\lfloor \frac{x}{m} \right\rfloor = \left\lfloor \frac{x}{b^{k-1}} \frac{b^{2k}}{m} \frac{1}{b^{k+1}} \right\rfloor$,

而（1）中$q_3 = \left\lfloor \left\lfloor \frac{x}{b^{k-1}} \right\rfloor \left\lfloor \frac{b^{2k}}{m} \right\rfloor \frac{1}{b^{k+1}} \right\rfloor$是$q$的估计。

显然$q_3 = \left\lfloor \left\lfloor \frac{x}{b^{k-1}} \right\rfloor \left\lfloor \frac{b^{2k}}{m} \right\rfloor \frac{1}{b^{k+1}} \right\rfloor \le q = \left\lfloor \frac{x}{b^{k-1}} \frac{b^{2k}}{m} \frac{1}{b^{k+1}} \right\rfloor$。

令$\alpha = \frac{x}{b^{k-1}} - \left\lfloor \frac{x}{b^{k-1}} \right\rfloor, \beta = \frac{b^{2k}}{m} - \left\lfloor \frac{b^{2k}}{m} \right\rfloor$

因此，$q = \left\lfloor \left(\left\lfloor \frac{x}{b^{k-1}} \right\rfloor + \alpha \right) \left(\left\lfloor \frac{b^{2k}}{m} \right\rfloor + \beta \right) \frac{1}{b^{k+1}} \right\rfloor$

$\le \left\lfloor \left\lfloor \frac{x}{b^{k-1}} \right\rfloor \left\lfloor \frac{b^{2k}}{m} \right\rfloor \frac{1}{b^{k+1}} + \left(\left\lfloor \frac{x}{b^{k-1}} \right\rfloor + \left\lfloor \frac{b^{2k}}{m} \right\rfloor + 1 \right) \frac{1}{b^{k+1}} \right\rfloor$

由于$\left\lfloor \frac{x}{b^{k-1}} \right\rfloor + \left\lfloor \frac{b^{2k}}{m} \right\rfloor + 1 \le b^{k+1} - 1 + b^{k+1} + 1 = 2b^{k+1}$

所以

$q \le \lfloor q_3 + 2 \rfloor = q_3 + 2$。

因此，$q - 2 \le q_3 \le q$。

而(2)中$-b^{k+1} < r_1 - r_2 < b^{k+1}$,

$r_1 - r_2 \equiv ((q - q_3)m + r)(\bmod b^{k+1})$

因为$m < b^k, b > 3$，所以$0 \le (q - q_3)m + r < 3m < b^{k+1}$。

若$r_1 - r_2 < 0$，则$r_1 - r_2 + b^{k+1} = (q - q_3)m + r$。这是(3)。

若$r_1 - r_2 \ge 0$，则$r_1 - r_2 = (q - q_3)m + r$。

#因为$0 \le r_1 - r_2 < 3m$，所以(4)最多重复2次。