MONTGOMERY REDUCTION

- Let us say that we want to compute $c = a \cdot b \bmod m$.
- The school book way is to compute $a \cdot b$ and follow it with a mod m. (The mod m part may be cumbersome)
- Montgomery showed how one could do a modular reduction without explicitly doing a mod m.

The steps are as follows.

① ~~Find R~~
Select R (generally a power of 2 s.t)
(a) $\gcd(R, m) = 1$
(b) R slightly greater than m.

② Use Extended Euclidean Algorithm to find R^{-1} & m' st.

$$R \cdot R^{-1} - mm' = 1$$

$$\text{or} \quad mm' \equiv -1 \bmod R \rightarrow mm' = (-1) + lR$$

(for some l)

③ Let $t = ab$

compute $\cdot$ $N = (t \cdot m' \bmod R)$

$$u = (t + Nm)/R$$

return $\underline{u}$ if $(u < m)$ or $\underline{(u-m)}$ if $(u \geq m)$

PROOF:

* First we show that $R \mid (t + Nm)$

$$N = tm' \bmod R = kR + tm' \quad (\text{for some } k)$$

$$\begin{aligned}(t+Nm) &= t + (kR + tm')m \\ &= t + kmR + tmm' \\ &= t + k'R + t((-1) + lR) \quad (k' = km) \\ &= \cancel{t} + k'R - \cancel{t} + tlR \\ &= \underline{qR}\end{aligned}$$

* Next we show that $uR = a \cdot b \bmod m$

$$uR = t + Nm$$
$$\equiv t \bmod m$$
$$= a \cdot b \bmod m$$

$\therefore$ ~~ok~~

Because of the addition $(t + Nm)$, the result will be at most $< 2m$.

The 'if' condition is therfore needed to reduce the result to less than m.

MONTGOMERY MULTIPLICATION EXAMPLE

Let's say we want to compute $a \cdot b \bmod m$

$a = 17$; $b = 26$; $m = 79$

the result is 47 $\qquad (17 \cdot 26 \bmod 79 = 47)$

- Choose $R = 100$ then as before

  $R^{-1} = 64$ $\quad m' = 81$ $\qquad 100(64) - 79(81) = 1$

- $\bar{a} = a \cdot R \bmod m = 41$

  $\bar{b} = b \cdot R \bmod m = 72$

Montgomery multiplication gives the result in Montgomery domain

ie $\bar{c} = (a \cdot b) R \bmod m$

$= \bar{a} R^{-1} \cdot \bar{b} R^{-1} \cdot R \bmod m$

$= \bar{a}\, \bar{b}\, R^{-1} \bmod m$

NOTE: This $\bar{c}$ should be $47 \cdot 100 \bmod 79 = 39$

and $c = \bar{c}\, R^{-1} \bmod m$

NOTE: $c = 39 \cdot 64 \bmod 79 = 47$

① $t = \bar{a}\,\bar{b}$

$= 41 \cdot 72 = 2952$ $\qquad t \bmod R = 52$

② $N = \cancel{29} \cdot t\, m' \bmod 100 = \cancel{24}$

$= 52 \cdot 81 \bmod 100 = 12$

③ $u = (t + Nm)/R$

$(2952 + 12 \cdot 79)/100$

$= 3900/100 = 39$

④ $\because 39 < 79$ return 39

This is $\bar{c}$

$$\boxed{\begin{array}{l} ①\ t = \bar{a}\bar{b} \\ ②\ N = t \bmod R \cdot m' \bmod R \\ ③\ u = (t + Nm)/R \\ ④\ \text{return } u \text{ if } u < m \\ \quad\ \text{else } (u - m) \end{array}}$$