Barrett Reduction

https://youtu.be/DzcysGAiDhw

한성대학교
HANSUNG UNIVERSITY

CryptoCraft LAB

Barrett Reduction

- 1986년 P.D. Barrett이 제안한 Classic Modular Multiplication 알고리즘
- 사전에 연산된 Barrett 상수를 사용하여 **곱셈과 뺄셈**만으로 주어진 값에 대한 나머지를 계산하는 기법
  - Modular Multiplication
    - 어떤 정수 a를 다른 정수 n으로 나누면 나오는 나머지

$$c = a \ \ mod \ \ n = a - qn \ (q\text{는 나눗셈의 몫})$$

$$(A \ {}^\wedge B)\ mod\ C = (A\ mod\ C \ * B\ mod\ C)\ mod\ C$$

Barrett Reduction

$$\frac{x}{m} = \left(\frac{1}{z} * \frac{x}{u/z}\right)\frac{u}{m}$$

$$= \frac{[x/(u/z)](u/m)}{z}$$

- Barret reduction의 주요 아이디어
  - $\frac{\boldsymbol{x}}{\boldsymbol{m}} \rightarrow \boldsymbol{x} * \frac{\boldsymbol{1}}{\boldsymbol{m}}$ **으로 대체**
  - $\frac{x}{m}$ 결과인 정수(근사값)을 얻고, x도 스케일링을 하기 위해서는 $\frac{1}{m}$에 대한 스케일링 필요

$$\frac{x}{m} = \frac{x}{u} * \frac{u}{m}$$

  - u 가 충분히 크면, $\frac{u}{m}$ 에 대한 정수(근사값)을 쉽게 얻을 수 있음.
  - u 가 매우 크면, $\frac{x}{m}$ 는 매우 작음 $\rightarrow u$ 에 대한 스케일링 필요 (임의의 z 만큼)

https://link.springer.com/chapter/10.1007/978-3-030-34142-8_4

Barrett Reduction

- Example
  - $x = 193\ by\ m = 13\ \rightarrow$ 몫 $q = 14$ 나머지 r = 11
    - $r = x\ mod\ m = 193\ mod\ 13$

  - $u = 200, z = 5$ 이라고 가정

  - $\frac{x(193)}{m(13)} = \frac{\mathrm{x}(193)}{u(200)} * \frac{\mathrm{u}(200)}{\mathrm{m}(13)}$ $(\frac{200}{13} = 15.385)$

  - $\frac{\mathrm{x}(193)}{u(200)} = \boxed{\frac{1}{z(5)} * \frac{\mathrm{x}(193)}{\frac{\mathrm{u}}{\mathrm{z}}(40)}}$ $(\frac{193}{40} = 4.825)$

  - $\frac{193}{13} = (\frac{193}{40} * \frac{200}{13})\ /\ 5$

$$\frac{x}{m} = \boxed{\frac{x}{u}} * \frac{u}{m}$$

$$\frac{x}{m} = \boxed{\left(\frac{1}{z} * \frac{x}{u/z}\right)} \frac{u}{m}$$

$$= \frac{[x/(u/z)](u/m)}{z}$$

Barrett Reduction

- Example
  - $x = 193\ by\ m = 13\ \rightarrow$ 몫 $q = 14$ 나머지 r = 11
    - $r = x\ mod\ m = 193\ mod\ 13$
  - $u = 200, z = 5$ 이라고 가정
  - $\tilde{q} = (4 * 5)/5$ = 12
  - $\tilde{r} = x - \tilde{q}m = 193 - 12 * 13 = 37$
    - $\tilde{r}$ = 37 로, m값보다 크기 때문에 수정 필요
  - $r = \tilde{r} - km = 37\ - 2 * 13 = 11\ (k = 2)$

$$\frac{x}{m} = \boxed{\frac{x}{u}} * \frac{u}{m}$$

$$\frac{x}{m} = \boxed{\left(\frac{1}{z} * \frac{x}{u/z}\right)}\frac{u}{m}$$

$$= \frac{[x/(u/z)](u/m)}{z}$$

Barrett Reduction

- $x = 2\text{n } bit \ (\text{x} < 2^{2n})(\ n = \lfloor \log_2 m \rfloor + 1 \ , \ \ x < m^2 \ \ , 2^{n-1} \leq m < 2^n \ )$
- $u = 2^{2n}, z = 2^{n+1}, \ \ \frac{\text{u}}{z} = \frac{2^{2n}}{2^{n+1}} = 2^{n-1}$

$$q = \left\lfloor \frac{x}{m} \right\rfloor$$

$$= \left\lfloor \boxed{\boxed{\frac{1}{2^{n+1}}} * \frac{x}{2^{n-1}}} * \frac{2^{2n}}{m} \right\rfloor$$

$$= \left\lfloor \frac{\left(x/2^{n-1}\right)\left(2^{2n}/m\right)}{\boxed{2^{n+1}}} \right\rfloor$$

$$\frac{x}{m} = \boxed{\left(\boxed{\frac{1}{z}} * \frac{x}{u/z}\right)} \frac{u}{m}$$

$$= \frac{[x/(u/z)](u/m)}{z}$$

$$\tilde{q} = \left\lfloor \frac{\lfloor x/2^{n-1} \rfloor * \lfloor 2^{2n}/m \rfloor}{2^{n+1}} \right\rfloor$$

$$\tilde{y} = x - \tilde{q}m$$

$$y = \begin{cases} \tilde{y} & \text{if } \tilde{y} < m \\ \tilde{y} - m & \text{if } m \leq \tilde{y} < 2m \\ \tilde{y} - 2m & \text{otherwise} \end{cases}$$

Barrett Reduction

- Example
- $x = 193, \;\; m = 1011_2 = 11, n = 2$

$$\left\lfloor \frac{x}{2^{n-1}} \right\rfloor = \left\lfloor \frac{193}{2^3} \right\rfloor = 11000_2 = 24$$

$$\left\lfloor \frac{2^{2n}}{m} \right\rfloor = \left\lfloor \frac{2^8}{11} \right\rfloor = 10111_2 = 23$$

$$24 * 23 = 551 = 1000\mathbf{01000}_2$$

$$\tilde{q} = \left\lfloor \frac{552}{2^5} \right\rfloor = 17 = 10001_2$$

$$\tilde{y} = 193 - 17 * 11 = 6$$

$$y = 6$$

$$q = \left\lfloor \frac{x}{m} \right\rfloor$$

$$= \left\lfloor \frac{1}{2^{n+1}} * \boxed{\frac{x}{2^{n-1}}} * \boxed{\frac{2^{2n}}{m}} \right\rfloor$$

$$= \left\lfloor \frac{\left(x/2^{n-1}\right)\left(2^{2n}/m\right)}{2^{n+1}} \right\rfloor$$

$$\frac{x}{m} = \frac{x}{u} * \frac{u}{m}$$

$$\frac{x}{m} = \left(\frac{1}{z} * \frac{x}{u/z}\right)\frac{u}{m}$$

$$= \frac{[x/(u/z)](u/m)}{z}$$

Barrett Reduction

$\lfloor a \rfloor$: a보다 작은 최대 정수

Table 1. Barrett reduction steps.

Algorithm 1. Barrett reduction
Input: integers $p, b \geq 3$, $k = \lfloor \log_b p \rfloor + 1, 0 \leq z \leq b^{2k}, \mu = \lfloor b^{2k}/p \rfloor$.
Output: $z \, mod \, p$.
1. $\boxed{\hat{q}} = \lfloor \lfloor z/b^{k-1} \rfloor \times \mu / b^{k+1} \rfloor$
2. $r = (z \bmod b^{K+1}) - (\hat{q} \times p \bmod b^{k+1})$
3. if $r < 0$, then $r = r + b^{k+1}$
4. repeat $r = r - p$ when $r \geq p$
5. return $\boxed{r.}$

몫의 근사값

나머지의 근사값
(결과값)

$$q = \left\lfloor \frac{x}{m} \right\rfloor$$

$$= \left\lfloor \frac{1}{2^{n+1}} * \frac{x}{2^{n-1}} * \frac{2^{2n}}{m} \right\rfloor$$

$$= \left\lfloor \frac{\left(x/2^{n-1}\right)\left(2^{2n}/m\right)}{2^{n+1}} \right\rfloor$$

$$\tilde{r} = x - \tilde{q}m$$
$$r = \tilde{r} - km$$

Q & A