Short-Limb Multiplication Techniques (Montgomery, Barrett...)

Bo-Yin Yang (with Matthias Kannwischer)

June 8, 2023 at Vodice

Modular Reductions

Barrett Reductions

Hensel Remainders and Montgomery Variations

Modular Reductions

Many cryptographic programs need $A \bmod M$, most often for a known M.

- For RSA and ECC, usually the numbers are multi-limb and unsigned.
- For postquantum cryptography (PQC) they are often single limb and signed.
- Often it is not necessarily that we have an exact $A \bmod M$, anything small that we can continue to compute with is okay.
  - At the end of the computation the canonical form is needed.
- There are two classes of approaches:

  Approximate Quotients: try straightforwardly to approximate $A \div M$

  Hensel Remainders: ...find exactly $AR \bmod M$ for some R (see below)

Barrett Reduction: Approximating Quotients

- For $A \bmod M = A - \lfloor A/M \rceil M$ (centered), $\lfloor A/M \rceil$ then obviously approximated

$$\lfloor A/M \rceil \quad \doteqdot \quad \lfloor A \times \lfloor 2^k/M \rceil / 2^k \rceil = (A \times \lfloor 2^k/M \rceil + 2^{k-1}) \gg k.$$ ($\gg$ is "shift".)

Barrett Reduction: Approximating Quotients

- For $A \bmod M = A - \lfloor A/M \rceil M$ (centered), $\lfloor A/M \rceil$ then obviously approximated

$$\lfloor A/M \rceil \quad \doteqdot \quad \lfloor A \times \lfloor 2^k/M \rceil / 2^k \rceil = (A \times \lfloor 2^k/M \rceil + 2^{k-1}) \gg k. \text{ (}\gg\text{ is “shift”.)}$$

- Suppose we instead want the unsigned $A \bmod M = A - \lfloor A/M \rfloor M$. Do we want

Barrett Reduction: Approximating Quotients

- For $A \bmod M = A - \lfloor A/M \rceil M$ (centered), $\lfloor A/M \rceil$ then obviously approximated

$$\lfloor A/M \rceil \;\doteqdot\; \lfloor A \times \lfloor 2^k/M \rceil / 2^k \rceil = (A \times \lfloor 2^k/M \rceil + 2^{k-1}) \gg k. \text{ (}\gg\text{ is “shift”.)}$$

- Suppose we instead want the unsigned $A \bmod M = A - \lfloor A/M \rfloor M$. Do we want
  - $\lfloor A/M \rfloor \doteqdot \lfloor A \times \lfloor 2^k/M \rfloor / 2^k \rfloor = (A \times \lfloor 2^k/M \rfloor) \gg k$? Then the approximate $A \bmod M$ is nonnegative, but returns a noncanonical M instead of 0 if we substitute M.

Barrett Reduction: Approximating Quotients

- For $A \bmod M = A - \lfloor A/M \rceil M$ (centered), $\lfloor A/M \rceil$ then obviously approximated

$$\lfloor A/M \rceil \quad \fallingdotseq \quad \lfloor A \times \lfloor 2^k/M \rceil / 2^k \rceil = (A \times \lfloor 2^k/M \rceil + 2^{k-1}) \gg k.$$ ($\gg$ is “shift”.)

- Suppose we instead want the unsigned $A \bmod M = A - \lfloor A/M \rfloor M$. Do we want
  - $\lfloor A/M \rfloor \fallingdotseq \lfloor A \times \lfloor 2^k/M \rfloor / 2^k \rfloor = (A \times \lfloor 2^k/M \rfloor) \gg k$? Then the approximate $A \bmod M$ is nonnegative, but returns a noncanonical M instead of 0 if we substitute M.
  - Or we use $\lfloor A/M \rfloor \fallingdotseq \lfloor A \times \lfloor 2^k/M \rceil / 2^k \rceil = (A \times \lceil 2^k/M \rceil) \gg k$? This might return a negative $A \bmod M$. In particular, where $A \times \lceil 2^k/M \rceil / 2^k$ is just above the integer a, or $A \gtrsim a \times 2^k / \lceil 2^k/M \rceil$, if simultaneously $A < aM$ then $A - \lfloor A \times \lfloor 2^k/M \rceil / 2^k \rceil M < 0$. This will take place if $a \times 2^k / \lceil 2^k/M \rceil < aM - 1$, or $a \geq \left\lceil \left(M - 2^k / \lceil 2^k/M \rceil\right)^{-1} \right\rceil$. Finally we get the bound $A \geq A_M = \left\lfloor \left\lceil \left(M - 2^k / \lceil 2^k/M \rceil\right)^{-1} \right\rceil 2^k / \lceil 2^k/M \rceil \right\rfloor$.

Barrett Reduction: Approximating Quotients

- For $A \bmod M = A - \lfloor A/M \rceil M$ (centered), $\lfloor A/M \rceil$ then obviously approximated

$$\lfloor A/M \rceil \quad \fallingdotseq \quad \lfloor A \times \lfloor 2^k/M \rceil / 2^k \rceil = (A \times \lfloor 2^k/M \rceil + 2^{k-1}) \gg k. \text{ (} \gg \text{ is “shift”.)}$$

- Suppose we instead want the unsigned $A \bmod M = A - \lfloor A/M \rfloor M$. Do we want
  - $\lfloor A/M \rfloor \fallingdotseq \lfloor A \times \lfloor 2^k/M \rfloor / 2^k \rfloor = (A \times \lfloor 2^k/M \rfloor) \gg k$? Then the approximate $A \bmod M$ is nonnegative, but returns a noncanonical M instead of 0 if we substitute M.
  - Or we use $\lfloor A/M \rfloor \fallingdotseq \lfloor A \times \lceil 2^k/M \rceil / 2^k \rceil = (A \times \lceil 2^k/M \rceil) \gg k$? This might return a negative $A \bmod M$. In particular, where $A \times \lceil 2^k/M \rceil / 2^k$ is just above the integer a, or $A \gtrsim a \times 2^k / \lceil 2^k/M \rceil$, if simultaneously $A < aM$ then $A - \lfloor A \times \lceil 2^k/M \rceil / 2^k \rfloor M < 0$. This will take place if $a \times 2^k / \lceil 2^k/M \rceil < aM - 1$, or $a \geq \left\lceil \left(M - 2^k / \lceil 2^k/M \rceil\right)^{-1} \right\rceil$. Finally we get the bound $A \geq A_M = \left\lceil \left\lceil \left(M - 2^k / \lceil 2^k/M \rceil\right)^{-1} \right\rceil 2^k / \lceil 2^k/M \rceil \right\rceil$.
    - Example: For $M = 4591$, $k = 32$, $a = 2161$, and $A_M = 9921150 (< M^2)$.
  - When out of bounds, needs to adjust (usually) by $\pm M$.

Barrett Reduction (examples)

- If $M = 4591$, $k = 32$, then $\overline{M} = \lfloor 2^k / M \rceil = 935519$
  - $2295 - 4591\lfloor 935519 \times 2295/2^{32} \rceil = 2295$
  - $2296 - 4591\lfloor 935519 \times 2296/2^{32} \rceil = -2295$
- If $M = 4591$, $k = 32$, then $\tilde{M} = \lceil 2^k / M \rceil = 935519$
  - $4591 - 4591\lfloor 935519 \times 4591/2^{32} \rfloor = 0$
  - $4590 - 4590\lfloor 935519 \times 4590/2^{32} \rfloor = 4590$, but
  - $-4591 - 4591\lfloor 935519 \times (-4591)/2^{32} \rfloor = 4591$
  - $9921150 - 4591\lfloor 935519 \times 9921150/2^{32} \rfloor = -1$

Note if we instead use $\lfloor 2^k / M \rfloor = 935518$, then we see

  - $4591 - 4591\lfloor 935518 \times 4591/2^{32} \rfloor = 4591$
  - $4592 - 4591\lfloor 935518 \times 4592/2^{32} \rfloor = 1$

Barrett Reduction (CPU-Specific Cases)

- ARMv7e-M has an SMMULR, easy to do centered Barrett on 32 bit
  $\text{SMMULR}(A, B) = (A \times B + 2^{31}) \gg 32$, so $\overline{M} = \lfloor 2^{32}/M \rceil$,
  and we have $\lfloor A/M \rceil \approx \text{SMMULR}(A, \overline{M})$
  Similarly ARMv7e-M has SMLAWx ($x = B, T$, Bottom / Top) instruction
  $\text{SMLAWx}(A, B, C) = \lfloor A \times B_x / 2^{16} \rfloor + C$, so
  $\pm\lfloor A_x/M \rceil \approx \text{SMLAWx}(\pm\overline{M}, A, 2^{15}) \gg 16$, similarly for unsigned case
  $\lfloor -A_x/M \rfloor \sim \text{SMLAWx}(-\tilde{M}, A, 2^{16}) \gg 16$, where $\tilde{M} = \lceil 2^{32}/M \rceil$.

Barrett Reduction (CPU-Specific Cases)

- ARMv7e-M has an SMMULR, easy to do centered Barrett on 32 bit
  $\mathrm{SMMULR}(A, B) = (A \times B + 2^{31}) \gg 32$, so $\overline{M} = \lfloor 2^{32}/M \rceil$,
  and we have $\lfloor A/M \rceil \approx \mathrm{SMMULR}(A, \overline{M})$
  Similarly ARMv7e-M has SMLAWx (x = B, T, Bottom / Top) instruction
  $\mathrm{SMLAWx}(A, B, C) = \lfloor A \times B_x / 2^{16} \rfloor + C$, so
  $\pm \lfloor A_x / M \rceil \approx \mathrm{SMLAWx}(\pm \overline{M}, A, 2^{15}) \gg 16$, similarly for unsigned case
  $\lfloor -A_x / M \rfloor \sim \mathrm{SMLAWx}(-\tilde{M}, A, 2^{16}) \gg 16$, where $\tilde{M} = \lceil 2^{32}/M \rceil$.
- X86 provides VPMULHRSW, computes $(X \times Y + 2^{14}) \gg 15$ (not very accurate.)

Barrett Reduction (CPU-Specific Cases)

- ARMv7e-M has an SMMULR, easy to do centered Barrett on 32 bit
  $\mathrm{SMMULR}(A, B) = (A \times B + 2^{31}) \gg 32$, so $\overline{M} = \lfloor 2^{32}/M \rceil$,
  and we have $\lfloor A/M \rceil \approx \mathrm{SMMULR}(A, \overline{M})$
  Similarly ARMv7e-M has SMLAWx (x = B, T, Bottom / Top) instruction
  $\mathrm{SMLAWx}(A, B, C) = \lfloor A \times B_x / 2^{16} \rfloor + C$, so
  $\pm\lfloor A_x / M \rceil \approx \mathrm{SMLAWx}(\pm\overline{M}, A, 2^{15}) \gg 16$, similarly for unsigned case
  $\lfloor -A_x / M \rfloor \sim \mathrm{SMLAWx}(-\tilde{M}, A, 2^{16}) \gg 16$, where $\tilde{M} = \lceil 2^{32}/M \rceil$.
- X86 provides VPMULHRSW, computes $(X \times Y + 2^{14}) \gg 15$ (not very accurate.)
- Many architectures has a multiply-return-high $Hi_k(A, B) = \lfloor A \times B / 2^k \rfloor$.
  Precompute $M' = \lfloor 2^{k+\ell}/M \rceil$, where $2^{\ell+1} > M > 2^{\ell}$. Then $\lfloor A/M \rceil \approx Hi_k(A, M') \gg \ell$

Error of Barrett Reductions $\mathrm{BAR}_M(z) = \mathrm{BAR}_M^{\lfloor\rceil}(z)$

We denote the approximation $\mathrm{BAR}_M^{\llbracket\rrbracket}(z) := z - \lfloor z \llbracket R/M \rrbracket / R \rceil$ **for suitable** R

$A \bmod M = A - \lfloor A/M \rfloor M$, $\mathrm{BAR}_M(A) = A - \lfloor A \lfloor 2^k/M \rceil / 2^k \rceil M$

- Let $\epsilon_0 = M \lfloor 2^k/M \rceil / 2^k - 1$, $\epsilon_1 = \lceil A \lfloor 2^k/M \rceil / 2^k \rfloor - A \lfloor 2^k/M \rceil / 2^k$, $\epsilon_2 = A/M - \lfloor A/M \rceil$

Error of Barrett Reductions $\mathrm{BAR}_M(z) = \mathrm{BAR}_M^{\lfloor\rceil}(z)$

We denote the approximation $\mathrm{BAR}_M^{[\![]\!]}(z) := z - \lfloor z [\![R/M]\!] /R \rceil$ **for suitable** R

$$A \bmod M = A - \lfloor A/M \rceil M, \ \mathrm{BAR}_M(A) = A - \lfloor A \lfloor 2^k/M \rceil / 2^k \rceil M$$

- Let $\epsilon_0 = M \lfloor 2^k/M \rceil / 2^k - 1$, $\epsilon_1 = \lceil A \lfloor 2^k/M \rceil / 2^k \rfloor - A \lfloor 2^k/M \rceil / 2^k$, $\epsilon_2 = A/M - \lfloor A/M \rceil$

$$\mathrm{Error} = A \bmod M - \mathrm{BAR}_M(A) = M(\lceil A \lceil 2^k/M \rfloor / 2^k \rfloor - \lceil A/M \rfloor)$$

Error of Barrett Reductions $\mathrm{BAR}_M(z) = \mathrm{BAR}_M^{\lfloor\rceil}(z)$

We denote the approximation $\mathrm{BAR}_M^{\llbracket\rrbracket}(z) := z - \lfloor z \llbracket R/M \rrbracket / R \rceil$ **for suitable** R

$$A \bmod M = A - \lfloor A/M \rceil M, \quad \mathrm{BAR}_M(A) = A - \lfloor A \lfloor 2^k/M \rceil / 2^k \rceil M$$

- Let $\epsilon_0 = M\lfloor 2^k/M \rceil / 2^k - 1$, $\epsilon_1 = \lceil A\lfloor 2^k/M \rceil / 2^k \rfloor - A\lfloor 2^k/M \rceil / 2^k$, $\epsilon_2 = A/M - \lfloor A/M \rceil$

$$\mathrm{Error} = A \bmod M - \mathrm{BAR}_M(A) = M(\lceil A\lceil 2^k/M \rfloor / 2^k \rfloor - \lceil A/M \rfloor)$$

$$= \quad M\left(\left(\lceil A\lfloor 2^k/M \rceil / 2^k \rfloor - A\lceil 2^k/M \rfloor / 2^k\right) + \left(A\lfloor 2^k/M \rceil / 2^k - \lceil A/M \rfloor\right)\right)$$

Error of Barrett Reductions $\mathrm{BAR}_M(z) = \mathrm{BAR}_M^{\lfloor\rceil}(z)$

We denote the approximation $\mathrm{BAR}_M^{[\![\,]\!]}(z) := z - \lfloor z\,[\![R/M]\!]\,/R\rceil$ **for suitable** R

$A \bmod M = A - \lfloor A/M\rceil M$, $\mathrm{BAR}_M(A) = A - \lfloor A\lfloor 2^k/M\rceil/2^k\rceil M$

- Let $\epsilon_0 = M\lfloor 2^k/M\rceil/2^k - 1$, $\epsilon_1 = \lceil A\lfloor 2^k/M\rceil/2^k\rfloor - A\lfloor 2^k/M\rceil/2^k$, $\epsilon_2 = A/M - \lfloor A/M\rceil$

$$
\begin{aligned}
\mathrm{Error} = A \bmod M - \mathrm{BAR}_M(A) &= M(\lceil A\lceil 2^k/M\rfloor/2^k\rfloor - \lceil A/M\rfloor) \\
= \quad & M\left(\left(\lceil A\lfloor 2^k/M\rceil/2^k\rfloor - A\lceil 2^k/M\rfloor/2^k\right) + \left(A\lfloor 2^k/M\rceil/2^k - \lceil A/M\rfloor\right)\right) \\
= \quad & M\left(\epsilon_1 + \left(A\lfloor 2^k/M\rceil/2^k - A/M\right) + (A/M - \lceil A/M\rfloor)\right) = M(\epsilon_1 + \epsilon_2) + A\epsilon_0
\end{aligned}
$$

- The first (two) terms are random errors and the last is a steady "drift" term.

Writing Down Explicit Extreme values of $\mathrm{BAR}_M(A)$

- We compute where, just before A, $A\lfloor 2^k/M\rceil/2^k$ last straddles a half-integer, which is $\tilde{A} = (\lceil A\lfloor 2^k/M\rceil/2^k + 0.5\rfloor - 0.5)\cdot 2^k/\lfloor 2^k/M\rceil$, or its $\lceil\ \rceil$ and $\lfloor\ \rfloor$, to compute the codomain, just computes the extremum value from $\{\mathrm{BAR}_M(A), \mathrm{BAR}_M(\lceil\tilde{A}\rceil), \mathrm{BAR}_M(\lfloor\tilde{A}\rfloor), \mathrm{BAR}_M(\lfloor-\tilde{A}\rfloor), \mathrm{BAR}_M(\lceil-\tilde{A}\rceil), \mathrm{BAR}_M(-A)\}$

Writing Down Explicit Extreme values of $\mathrm{BAR}_M(A)$

- We compute where, just before A, $A\lfloor 2^k/M\rceil/2^k$ last straddles a half-integer, which is $\tilde{A} = (\lceil A\lfloor 2^k/M\rceil/2^k + 0.5\rfloor - 0.5) \cdot 2^k/\lfloor 2^k/M\rceil$, or its $\lceil\ \rceil$ and $\lfloor\ \rfloor$, to compute the codomain, just computes the extremum value from $\{\mathrm{BAR}_M(A), \mathrm{BAR}_M(\lceil\tilde{A}\rceil), \mathrm{BAR}_M(\lfloor\tilde{A}\rfloor), \mathrm{BAR}_M(\lfloor-\tilde{A}\rfloor), \mathrm{BAR}_M(\lceil-\tilde{A}\rceil), \mathrm{BAR}_M(-A)\}$
- Example: range of Barrett reduction for

$$k = 32,\quad A = 2^{31},\quad M = 4591 \quad \text{is} \quad \pm 2512$$
$$k = 32,\quad A = 2^{32},\quad M = 4591 \quad \text{is} \quad \pm 2721$$
$$k = 15,\quad A = 2^{15},\quad M = 4591 \quad \text{is} \quad \pm 2881$$

Writing Down Explicit Extreme values of $\mathrm{BAR}_M(A)$

- We compute where, just before A, $A\lfloor 2^k/M\rceil/2^k$ last straddles a half-integer, which is $\tilde{A} = (\lceil A\lfloor 2^k/M\rceil/2^k + 0.5\rfloor - 0.5)\cdot 2^k/\lfloor 2^k/M\rceil$, or its $\lceil\ \rceil$ and $\lfloor\ \rfloor$, to compute the codomain, just computes the extremum value from $\{\mathrm{BAR}_M(A), \mathrm{BAR}_M(\lceil\tilde{A}\rceil), \mathrm{BAR}_M(\lfloor\tilde{A}\rfloor), \mathrm{BAR}_M(\lfloor-\tilde{A}\rfloor), \mathrm{BAR}_M(\lceil-\tilde{A}\rceil), \mathrm{BAR}_M(-A)\}$
- Example: range of Barrett reduction for

$$\begin{array}{llll} k = 32, & A = 2^{31}, & M = 4591 & \text{is} \quad \pm 2512 \\ k = 32, & A = 2^{32}, & M = 4591 & \text{is} \quad \pm 2721 \\ k = 15, & A = 2^{15}, & M = 4591 & \text{is} \quad \pm 2881 \end{array}$$

- Similarly, for unsigned Barrett, we find $\tilde{A} = \lfloor A\lceil 2^k/M\rceil/2^k\rfloor \cdot 2^k/\lceil 2^k/M\rceil$ and proceed similarly with the points $A, \lceil\tilde{A}\rceil, \lfloor\tilde{A}\rfloor, \lceil-\tilde{A}\rceil, \lfloor-\tilde{A}\rfloor, -A$.

Range where Signed Barrett Reduction is Canonical

The max $|A|$ when $\mathrm{BAR}_M(A) = A - \lfloor A\lfloor 2^k/M\rceil/2^k\rceil$ is guaranteed to $= A - \lfloor A/M\rceil M$?

- for A/M and $\lfloor A\lfloor 2^k/M\rceil/2^k\rceil$ to agree, we just need

$$\delta := \left|A/M - \lfloor A\lfloor 2^k/M\rceil/2^k\rceil\right| < 1/(2M)$$

because $\lfloor\cdot\rceil$ only changes value at $\mathbb{Z} + \frac{1}{2}$.

Range where Signed Barrett Reduction is Canonical

The max $|A|$ when $\mathrm{BAR}_M(A) = A - \lfloor A \lfloor 2^k/M \rceil / 2^k \rceil$ is guaranteed to $= A - \lfloor A/M \rceil M$?

- for A/M and $\lfloor A \lfloor 2^k/M \rceil / 2^k \rceil$ to agree, we just need

$$\delta := \left| A/M - \lfloor A \lfloor 2^k/M \rceil / 2^k \rceil \right| < 1/(2M)$$

  because $\lfloor \cdot \rceil$ only changes value at $\mathbb{Z} + \frac{1}{2}$.
- $\delta < (A/2^k) \left| \lfloor 2^k/M \rceil - 2^k/M \right| = (A/M)|\varepsilon_0|$, therefore $\mathrm{BAR}_M(A) = A \bmod M$ is guaranteed if $A < 1/(2|\varepsilon_0|)$.

  Example: Barrett reduction is canonical for

  $k = 32,\quad M = 4591\quad$ then $\quad \varepsilon_0 = 1.01 \times 10^{-7},\quad A \lesssim 5 \times 10^6$

  $k = 31,\quad M = 4591\quad$ then $\quad \varepsilon_0 = -0.97 \times 10^{-7},\quad A \lesssim 5 \times 10^6$

Range where Signed Barrett Reduction is Canonical

The max $|A|$ when $\mathrm{BAR}_M(A) = A - \lfloor A\lfloor 2^k/M\rceil/2^k\rceil$ is guaranteed to $= A - \lfloor A/M\rceil M$?

- for A/M and $\lfloor A\lfloor 2^k/M\rceil/2^k\rceil$ to agree, we just need

  $$\delta := \left|A/M - \lfloor A\lfloor 2^k/M\rceil/2^k\right| < 1/(2M)$$

  because $\lfloor\cdot\rceil$ only changes value at $\mathbb{Z} + \frac{1}{2}$.
- $\delta < (A/2^k)\left|\lfloor 2^k/M\rceil - 2^k/M\right| = (A/M)|\varepsilon_0|$, therefore $\mathrm{BAR}_M(A) = A \bmod M$ is guaranteed if $A < 1/(2|\varepsilon_0|)$.

  Example: Barrett reduction is canonical for

  $k = 32,\quad M = 4591\quad \text{then}\quad \varepsilon_0 = 1.01 \times 10^{-7},\quad A \lesssim 5 \times 10^6$

  $k = 31,\quad M = 4591\quad \text{then}\quad \varepsilon_0 = -0.97 \times 10^{-7},\quad A \lesssim 5 \times 10^6$

Range where Signed Barrett Reduction is Canonical

The max $|A|$ when $\mathrm{BAR}_M(A) = A - \lfloor A \lfloor 2^k/M \rceil / 2^k \rceil$ is guaranteed to $= A - \lfloor A/M \rceil M$?

- for A/M and $\lfloor A \lfloor 2^k/M \rceil / 2^k \rceil$ to agree, we just need

$$\delta := \left| A/M - \lfloor A \lfloor 2^k/M \rceil / 2^k \rceil \right| < 1/(2M)$$

  because $\lfloor \cdot \rceil$ only changes value at $\mathbb{Z} + \frac{1}{2}$.
- $\delta < (A/2^k) \left| \lfloor 2^k/M \rceil - 2^k/M \right| = (A/M)|\varepsilon_0|$, therefore
  $\mathrm{BAR}_M(A) = A \bmod M$ is guaranteed if $A < 1/(2|\varepsilon_0|)$.
  Example: Barrett reduction is canonical for

$$k = 32, \quad M = 4591 \quad \text{then} \quad \varepsilon_0 = 1.01 \times 10^{-7}, \quad A \lesssim 5 \times 10^6$$

$$k = 31, \quad M = 4591 \quad \text{then} \quad \varepsilon_0 = -0.97 \times 10^{-7}, \quad A \lesssim 5 \times 10^6$$

- for unsigned Barrett we often don't have such luxuries.

Montgomery Reduction (Signed, for M odd)

- We want A mod M, but Barrett reduction requires full-length (double-length, depending on PoV) multiplications, can we do better?

Montgomery Reduction (Signed, for M odd)

- We want $A \bmod M$, but Barrett reduction requires full-length (double-length, depending on PoV) multiplications, can we do better?
- Answer by Peter Montgomery: let's compute not $A \bmod M$, but $A/R \bmod M$, where R is something that is easy to divide by (typically power of 2)

Montgomery Reduction (Signed, for M odd)

- We want $A \bmod M$, but Barrett reduction requires full-length (double-length, depending on PoV) multiplications, can we do better?
- Answer by Peter Montgomery: let's compute not $A \bmod M$, but $A/R \bmod M$, where R is something that is easy to divide by (typically power of 2)
- Compute $M' = 1/M \bmod R$ given A, compute $\ell = AM' \bmod R$ (as $(A \bmod R)M' \bmod R$) then $\ell M \equiv AM'M \equiv A \pmod R$

Montgomery Reduction (Signed, for M odd)

- We want $A \bmod M$, but Barrett reduction requires full-length (double-length, depending on PoV) multiplications, can we do better?
- Answer by Peter Montgomery: let's compute not $A \bmod M$, but $A/R \bmod M$, where R is something that is easy to divide by (typically power of 2)
- Compute $M' = 1/M \bmod R$ given A, compute $\ell = AM' \bmod R$ (as $(A \bmod R)M' \bmod R$) then $\ell M \equiv AM'M \equiv A \pmod R$
- So we compute $A - \ell M$, this is divisible by R, hence, $(A - \ell M)/R \equiv A/R \pmod M$ because $(A - \ell M)/R \cdot R = A - \ell M \equiv A \pmod M$, and $\gcd(M, R) = 1$

Montgomery Reduction (Signed, for M odd)

- We want $A \bmod M$, but Barrett reduction requires full-length (double-length, depending on PoV) multiplications, can we do better?
- Answer by Peter Montgomery: let's compute not $A \bmod M$, but $A/R \bmod M$, where R is something that is easy to divide by (typically power of 2)
- Compute $M' = 1/M \bmod R$ given A, compute $\ell = AM' \bmod R$ (as $(A \bmod R)M' \bmod R$) then $\ell M \equiv AM'M \equiv A \pmod{R}$
- So we compute $A - \ell M$, this is divisible by R, hence, $(A - \ell M)/R \equiv A/R \pmod{M}$ because $(A - \ell M)/R \cdot R = A - \ell M \equiv A \pmod{M}$, and $\gcd(M, R) = 1$
  - For $(A - \ell M)/R$ we need not the bottom half of ℓM, just the top half.

Examples of (Signed) Montgomery Reduction

- Let $M = 83$, $R = 100$, Now we wish to compute the (signed) Montgomery reduction of $A = 6412$. We know that $M' = 1/M \bmod R = 47$. now $\ell = (A \bmod R)M' \bmod R = 12 \times 47 \bmod 100 = -36$ (centered or lifted mod). $A - \ell M = 6412 - (-36) \times 83 = 6412 - (-2988) = 9400$, so we get 94.
  - Montgomery does not guarantee the canonical value: $6412 \cong 1100 \pmod{83}$.

Examples of (Signed) Montgomery Reduction

- Let $M = 83, R = 100$, Now we wish to compute the (signed) Montgomery reduction of $A = 6412$. We know that $M' = 1/M \bmod R = 47$. now $\ell = (A \bmod R)M' \bmod R = 12 \times 47 \bmod 100 = -36$ (centered or lifted mod). $A - \ell M = 6412 - (-36) \times 83 = 6412 - (-2988) = 9400$, so we get 94.
  - Montgomery does not guarantee the canonical value: $6412 \cong 1100 \pmod{83}$.
- Suppose we want the Montgomery reduction of $A = 3322$, then $\ell = 22 \times 47 \bmod 100 = 34$, and $A - \ell M = 3322 - 34 \times 87 = 500$, and we get 5.

Examples of (Signed) Montgomery Reduction

- Let $M = 83, R = 100$, Now we wish to compute the (signed) Montgomery reduction of $A = 6412$. We know that $M' = 1/M \bmod R = 47$. now $\ell = (A \bmod R)M' \bmod R = 12 \times 47 \bmod 100 = -36$ (centered or lifted mod). $A - \ell M = 6412 - (-36) \times 83 = 6412 - (-2988) = 9400$, so we get 94.
  - Montgomery does not guarantee the canonical value: $6412 \cong 1100 \pmod{83}$.
- Suppose we want the Montgomery reduction of $A = 3322$, then $\ell = 22 \times 47 \bmod 100 = 34$, and $A - \ell M = 3322 - 34 \times 87 = 500$, and we get 5.
- M' is computable on the fly via Hensel Lifting:

Examples of (Signed) Montgomery Reduction

- Let $M = 83, R = 100$, Now we wish to compute the (signed) Montgomery reduction of $A = 6412$. We know that $M' = 1/M \bmod R = 47$. now $\ell = (A \bmod R)M' \bmod R = 12 \times 47 \bmod 100 = -36$ (centered or lifted mod). $A - \ell M = 6412 - (-36) \times 83 = 6412 - (-2988) = 9400$, so we get 94.
  - Montgomery does not guarantee the canonical value: $6412 \cong 1100 \pmod{83}$.
- Suppose we want the Montgomery reduction of $A = 3322$, then $\ell = 22 \times 47 \bmod 100 = 34$, and $A - \ell M = 3322 - 34 \times 87 = 500$, and we get 5.
- M' is computable on the fly via Hensel Lifting:
  - Say $M = 47, R = 256 = 2^8$, for $x = 1/M \pmod{256}$, set $x_0 = 1 \equiv x \pmod{2}$, then

Examples of (Signed) Montgomery Reduction

- Let $M = 83$, $R = 100$, Now we wish to compute the (signed) Montgomery reduction of $A = 6412$. We know that $M' = 1/M \bmod R = 47$. now $\ell = (A \bmod R)M' \bmod R = 12 \times 47 \bmod 100 = -36$ (centered or lifted mod). $A - \ell M = 6412 - (-36) \times 83 = 6412 - (-2988) = 9400$, so we get 94.
  - Montgomery does not guarantee the canonical value: $6412 \cong 1100 \pmod{83}$.
- Suppose we want the Montgomery reduction of $A = 3322$, then $\ell = 22 \times 47 \bmod 100 = 34$, and $A - \ell M = 3322 - 34 \times 87 = 500$, and we get 5.
- M' is computable on the fly via Hensel Lifting:
  - Say $M = 47$, $R = 256 = 2^8$, for $x = 1/M \pmod{256}$, set $x_0 = 1 \equiv x \pmod{2}$, then

$$x_1 \equiv 2x_0 - x_0^2 M \equiv -45 \equiv -1 \equiv x \pmod{4}; \qquad x_2 \equiv 2x_1 - x_1^2 M \equiv -1 \equiv x \pmod{16};$$

$$x_3 \equiv 2x_2 - x_2^2 M \equiv -49 \equiv x \pmod{256}.$$

Unsigned (Original) Montgomery Reduction

- A is unsigned: now we let $M' = -1/M \pmod{R}$
  $\ell = M'(A \bmod R) \bmod R$, so $A + \ell M = 0 \pmod{R}$
  hence $(A + \ell M)/R = A/R \pmod{M}$

Unsigned (Original) Montgomery Reduction

- A is unsigned: now we let $M' = -1/M \pmod{R}$
  $\ell = M'(A \bmod R) \bmod R$, so $A + \ell M = 0 \pmod{R}$
  hence $(A + \ell M)/R = A/R \pmod{M}$
- Suppose we wish to compute the *unsigned* Montgomery Reduction of 6412 and 3322 as above, then $M' = -1/M \bmod R = 53$.
  - The reduction of 6412 is $(6412 + (53 \times 12 \bmod 100) \times 83)/100 = 94$ as before.
  - The reduction of 3322 is $3322 + (53 \times 22 \bmod 100) \times 83 = 88 \neq 5$.

Unsigned (Original) Montgomery Reduction

- A is unsigned: now we let $M' = -1/M \pmod{R}$
  $\ell = M'(A \bmod R) \bmod R$, so $A + \ell M = 0 \pmod{R}$
  hence $(A + \ell M)/R = A/R \pmod{M}$
- Suppose we wish to compute the *unsigned* Montgomery Reduction of 6412 and 3322 as above, then $M' = -1/M \bmod R = 53$.
  - The reduction of 6412 is $(6412 + (53 \times 12 \bmod 100) \times 83)/100 = 94$ as before.
  - The reduction of 3322 is $3322 + (53 \times 22 \bmod 100) \times 83 = 88 \neq 5$.
- Pros and Cons:
  - pluses: deals with unsigned numbers, so can do multiprecision

Unsigned (Original) Montgomery Reduction

- A is unsigned: now we let $M' = -1/M \pmod{R}$
  $\ell = M'(A \bmod R) \bmod R$, so $A + \ell M = 0 \pmod{R}$
  hence $(A + \ell M)/R = A/R \pmod{M}$
- Suppose we wish to compute the *unsigned* Montgomery Reduction of 6412 and 3322 as above, then $M' = -1/M \bmod R = 53$.
  - The reduction of 6412 is $(6412 + (53 \times 12 \bmod 100) \times 83)/100 = 94$ as before.
  - The reduction of 3322 is $3322 + (53 \times 22 \bmod 100) \times 83 = 88 \neq 5$.
- Pros and Cons:
  - pluses: deals with unsigned numbers, so can do multiprecision
  - minuses: larger numbers, full-length addition for $A + \ell M$

Range under Montgomery Reduction (heretofore "MR")

- $|\mathrm{MR}(A)| = |(A - \ell M)|/R \leq |A/R| + M|\ell/R| \leq |A|/R + M/2$
  since we can compute in signed mod (centered mod)

Range under Montgomery Reduction (heretofore "MR")

- $|\mathrm{MR}(A)| = |(A - \ell M)|/R \le |A/R| + M|\ell/R| \le |A|/R + M/2$ since we can compute in signed mod (centered mod)
- Corollary: for $|A| < RM/2$, $|\mathrm{MR}(A)| < M$

Range under Montgomery Reduction (heretofore “MR”)

- $|\mathrm{MR}(A)| = |(A - \ell M)|/R \le |A/R| + M|\ell/R| \le |A|/R + M/2$
  since we can compute in signed mod (centered mod)
- Corollary: for $|A| < RM/2$, $|\mathrm{MR}(A)| < M$
- for unsigned Montgomery (we use $M' = -1/M \bmod R$ instead) and compute

$$|\mathrm{MR}(A)| = |A + \ell M|/R \le |A/R| + M\ell/R$$

$$\le |A|/R + M \le 2M, \qquad \text{provided that } A < RM.$$

Range under Montgomery Reduction (heretofore "MR")

- $|\mathrm{MR}(A)| = |(A - \ell M)|/R \le |A/R| + M|\ell/R| \le |A|/R + M/2$
  since we can compute in signed mod (centered mod)
- Corollary: for $|A| < RM/2$, $|\mathrm{MR}(A)| < M$
- for unsigned Montgomery (we use $M' = -1/M \bmod R$ instead) and compute

$$|\mathrm{MR}(A)| = |A + \ell M|/R \le |A/R| + M\ell/R$$
$$\le |A|/R + M \le 2M, \quad \text{provided that } A < RM.$$

- Note: bounds are smaller than M and $2M$ when A is smaller.

Montgomery Multiplication (1)

- if b is known, then we compute ab by computing $\mathrm{MR}(a \cdot (bR \bmod M))$ where $bR \bmod M$ is precomputed.

Montgomery Multiplication (1)

- if b is known, then we compute ab by computing $\mathrm{MR}(a \cdot (bR \bmod M))$ where $bR \bmod M$ is precomputed.
- On architectures where ”top half of products” and ”bottom half of products” are separate, we can even optimize to (all mods here are mod$^{\pm}$, centered).

$$\begin{aligned}
\mathrm{Mont}_M(a, b) &= \mathrm{MR}(a \cdot (bR \bmod M)) \\
&= [a(bR \bmod M) - ((a \cdot (bR \bmod M) \bmod R) \cdot M' \bmod R) \cdot M]/R \\
&= [a \cdot (bR \bmod M) - M \cdot (a \cdot M' \cdot (bR' \bmod M) \bmod R)]/R \\
&= \mathrm{Mulhi}[aB] - \mathrm{Mulhi}[M \cdot \mathrm{Mullo}[aB']]
\end{aligned}$$

where $B = (bR \bmod M)$, $B' = (BM' \bmod R)$

Montgomery Multiplication (2)

Equivalence of Montgomery Reduction with Barrett Reduction

$$\left[\!\left[\frac{R}{M}\right]\!\right] \textbf{ mod}^{\pm} R = \left(-(R \textbf{ mod}^{[\![\,]\!]} M)\cdot(M^{-1} \textbf{ mod}^{\pm} R)\right) \textbf{mod}^{\pm} R$$

Proof: $M\left[\!\left[\frac{R}{M}\right]\!\right] = R - R \bmod^{[\![\,]\!]} M$, take $\bmod^{\pm} R$ and multiply by $M^{-1} \bmod^{\pm} R$

$\mathrm{BAR}_M^{[\![\,]\!]}(z) = MR(z(R \textbf{ mod}^{[\![\,]\!]} M))$, **in particular** $\mathrm{BAR}_M(z) = MR(z(R \textbf{ mod}^{\pm} M))$

$$\begin{aligned}
\mathrm{BAR}_M^{[\![\,]\!]}(z) &= z - M\left\lfloor z\left[\!\left[\frac{R}{M}\right]\!\right]\right\rceil = z - \frac{M}{R}\left(z\left[\!\left[\frac{R}{M}\right]\!\right] - (z\left[\!\left[\frac{R}{M}\right]\!\right]) \bmod^{\pm} R\right) \\
&= z - \frac{1}{R}\left\{zM\left[\!\left[\frac{R}{M}\right]\!\right] - M\left[\left(-z(R \bmod^{[\![\,]\!]} M)\cdot(M^{-1} \bmod^{\pm} R)\right) \bmod^{\pm} R\right]\right\} \\
&= \frac{1}{R}\left\{z(R \bmod^{[\![\,]\!]} M) + M\left[-z(R \bmod^{[\![\,]\!]} M)(M^{-1} \bmod^{\pm} R) \bmod^{\pm} R\right]\right\}
\end{aligned}$$

Montgomery Multiplication (2, Continued)

Equivalence of Montgomery Multiplication with Barrett Multiplication

$$\mathrm{BAR}_M^{\llbracket\rrbracket}(A,B) := AB - M\left\lfloor A \left\llbracket \frac{BR}{M} \right\rrbracket \right\rceil = MR(A(BR \ \mathbf{mod}^{\llbracket\ \rrbracket}\ M))$$

Note that $\left\llbracket \frac{BR}{M} \right\rrbracket \bmod^{\pm} R = \left(-(BR \bmod^{\llbracket\ \rrbracket} M)\cdot(M^{-1} \bmod^{\pm} R)\right) \bmod^{\pm} R$ as above.

$$\begin{aligned}
\mathrm{BAR}_M^{\llbracket\rrbracket}(A,B) &= AB - M\left\lfloor A \left\llbracket \frac{BR}{M} \right\rrbracket \right\rceil = AB - \frac{M}{R}\left(A\left\llbracket \frac{BR}{M} \right\rrbracket - \left(A\left\llbracket \frac{BR}{M} \right\rrbracket\right) \bmod^{\pm} R\right) \\
&= AB - \frac{1}{R}\left\{AM\left\llbracket \frac{BR}{M} \right\rrbracket - M\left[\left(-A(BR \bmod^{\llbracket\ \rrbracket} M)\cdot(M^{-1} \bmod^{\pm} R)\right) \bmod^{\pm} R\right]\right\} \\
&= A - \frac{1}{R}\left\{AM\frac{BR-(BR \bmod^{\llbracket\ \rrbracket} M)}{M} - M\left[\left(-A(BR \bmod^{\llbracket\ \rrbracket} M)(M^{-1} \bmod^{\pm} R)\right) \bmod^{\pm} R\right]\right\} \\
&= \frac{1}{R}\left\{A(BR \bmod^{\llbracket\ \rrbracket} M) + M\left[-A(BR \bmod^{\llbracket\ \rrbracket} M)(M^{-1} \bmod^{\pm} R) \bmod^{\pm} R\right]\right\}
\end{aligned}$$

Montgomery Multiplication (2)

Now, we can do the following: (denote $B'' = (B'M - B) \gg 32$):

$$\begin{aligned}
\text{MM}(ab) &= \text{Mulhi}(aB) - \text{Mulhi}(M \cdot \text{Mullo}(aB')) \\
&= \lfloor aB/R \rfloor - \lfloor M \left(aB' \bmod^{\pm} R\right)/R \rfloor \\
&= \lfloor aB/R \rfloor - \lfloor M\,(aB' - \lfloor aB'/R \rceil R)/R \rfloor \\
&= \lfloor aB/R \rfloor - \lfloor aB'M/R \rfloor + M \lfloor aB'/R \rceil \\
&= -a \cdot (B'M - B)/R + M \cdot \lfloor aB'/R \rceil = -aB'' + M \cdot \lfloor aB'/R \rceil
\end{aligned}$$

which is bounded in absolute value by $|a||B|/R + M/2 < |a|/2 + M/2$ if $|B| < R/2$.

The reason for doing this

But, **why**? Certain microarchitectures can do both $\lceil aB'/R \rfloor$, and multiply-and-accumulate. Example: ARM's NEON has $\texttt{SQRDMULH}(x, y) = \lceil xy/2^{31} \rfloor$ so $\lceil aB'/R \rfloor = \texttt{SQRDMULH}(a, B'/2)$ if we take care to pick B (and hence B') even. Note that

- $B'' = \mathrm{MR}(-B) \equiv -B/R \equiv -b \pmod{M}$.
- $\lceil bR/M \rfloor = -B'$. Because

$$\lceil bR/M \rfloor = (bR - B)/M \equiv -B/M \equiv -BM' \equiv -B' \pmod{R}.$$

But $B' \in [-R/2, R/2)$ and so is $\lceil bR/M \rfloor$.

Montgomery Multiplication (2): Equivalence to Barrett

$$\mathrm{BAR}_M(ab) = ab - M\lfloor ab\lfloor R/M\rceil/R\rceil \approx ab - M\lfloor a\lfloor bR/M\rceil/R\rceil \approx -aB'' + M\lfloor aB'/R\rceil.$$

Can we prove that the two are equivalent? We can because $B = bR \bmod^{\pm} M$.

- Given $B'' = (B'M - B)/R$ is the same as $\mathrm{MR}(-B) \equiv -B/R \equiv -b \pmod{M}$, we know that B'' is a representative of $-b \pmod{M}$. But which? $B''R = B'M - B$, where $|B| < M$, so if $|B'| < R/2$, max of $|B''|$ is $((R/2-1)M + M - 1)/R = (RM/2-1)/R < M/2$. But if $B' = -R/2$, then from $B' = BM' \bmod^{\pm} R$ and M' being odd we know that $B \equiv -R/2 \pmod{R}$, which is impossible when $R > M$ and $B = bR \bmod^{\pm} M$, Therefore $-b = B''$ when $|b| < M/2$.

[Becker et al CHES 2022] Barrett (Signed Shoup) Multiplication

$\mathrm{BAR}_M^{[\![]\!]}(A,B) := AB - \lfloor A [\![B \cdot 2^k/M]\!] /2^k \rceil M$, **we omit** B **if 1, this is Barrett Reduction if** $B = 1$ **and** $[\![\cdot]\!] := \lfloor \cdot \rceil$

Barrett Multiplication, a recap

Let $M \in \mathbb{N}$ be odd and $A, B \in \mathbb{Z}$ with $|A|, |B| < 2^{\ell-1}$ for $\ell \in \{16, 32\}$. Moreover, let $[\![-]\!] : \mathbb{Q} \to \mathbb{Z}$ be any integer approximation, i.e. $|x - [\![x]\!]| \le 1$ for all $x \in \mathbb{Q}$, and put $t \bmod^{[\![]\!]} M := t - q\,[\![t/q]\!]$ and $\mathrm{BAR}_M^{[\![]\!]}(A,B) = AB - M\left\lfloor A\left[\!\!\left[\frac{B\cdot 2^k}{M}\right]\!\!\right]/2^k\right\rceil$. Then for $R := 2^k$, $|\mathrm{BAR}_M^{[\![]\!]}(A,B)| \le \frac{A(BR \bmod^{[\![\ ]\!]} M)}{R} + \frac{R}{2}$

Accuracy for (Rounding) Barrett Multiplication

Take max h with $\varepsilon := |\lfloor BR/M \rceil - BR/M| \le 2^{-h}$, and $R := 2^k$ where $k := (\ell - 1) + \lfloor \log_2 M \rfloor - \lceil \log_2 |B| \rceil$, then $\mathrm{BAR}_M^{\lfloor\cdot\rceil}(A,B) = AB \bmod^{\pm} M$, if $\log_2 |A| < (\ell - 1) - \lceil \log_2 |B| \rceil - (h - 1)$

(Signed) Plantard Multiplication

Useful only on an ARM Cortex-M4 with `SMULWx`, `SMLAWx`

We denote by $[A]^\ell$ and $[A]_\ell$ the numbers $\lfloor A/2^\ell \rfloor$ and $A \bmod^\pm 2^\ell$ respectively.

[Huang et al CHES 2022] Algorithm for odd positive q (positive integer α)

Input: signed integers $a, b \in [-q2^\alpha, q2^\alpha]$. $q < 2^{\ell-\alpha-1}$, $q' = q^{-1} \bmod^\pm 2^{2\ell}$.

Output: $c = \left[\left(\left[[abq']_{2\ell}\right]^\ell + 2^\alpha\right) q\right]^\ell$, $c = ab(-2^{-2\ell}) \bmod^\pm q$ where $c \in (-\frac{q}{2}, \frac{q}{2})$

$c \le \left\lfloor (2^{\ell-1} - 1 + 2^\alpha) q / 2^\ell \right\rfloor = \left\lfloor (q-1)/2 + \left(1/2 + (2^\alpha - 1) q / 2^\ell\right) \right\rfloor = \lfloor q/2 \rfloor$

let $p = abq^{-1} \bmod^\pm 2^{2\ell}$, $p_1 = \left\lfloor \frac{p}{2^\ell} \right\rfloor$. $p_0 = p - p_1 2^\ell$, then if $0 < q2^{\ell+\alpha} - p_0 q + ab < 2^{2\ell}$,

then $ab(-2^{-2\ell}) \overset{\bmod q}{\equiv} (pq - ab)/2^{2\ell} = \left\lfloor \frac{pq-ab}{2^{2\ell}} + \frac{q2^{\ell+\alpha} - p_0 q + ab}{2^{2\ell}} \right\rfloor = \left\lfloor (p_1 + 2^\alpha) q / 2^\ell \right\rfloor = c$. But

$0 < q\left(2^{\ell+\alpha-1} - 2^\ell\right) < q\left(2^{\ell+\alpha} - 2^\ell - q2^{2\alpha}\right) < q2^{\ell+\alpha} - p_0 q + ab < q2^{\ell+\alpha} + ab < (3/4)2^{2\ell}$.

(Signed) Plantard Multiplication (how to see it)

Alt. Algorithm for odd positive q (and positive integer $\bar{q} > 1$ s.t. $\bar{q}q < 2^{\ell-1}$)

Input: signed integers $a, b \in [-q\bar{q}, q\bar{q}]$. $q' = q^{-1} \bmod^{\pm} 2^{2\ell}$.

Output: $c = \left\lfloor \left(\left\lfloor [abq']_{2\ell} \right\rfloor^{\ell} + \bar{q} \right) q \right\rfloor^{\ell}$, $c = ab(-2^{-2\ell}) \bmod^{\pm} q$ where $c \in (-\frac{q}{2}, \frac{q}{2})$

let $p = abq^{-1} \bmod^{\pm} 2^{2\ell}$, $p_1 = \left\lfloor \frac{p}{2^{\ell}} \right\rfloor \in [-2^{\ell-1}; 2^{\ell-1} - 1]$, $p_0 = p - p_1 2^{\ell} \in [0; 2^{\ell} - 1]$.

So $-ab2^{-2\ell} \equiv (pq - ab)/2^{2\ell} \equiv \frac{p_1 q}{2^{\ell}} - \frac{ab - p_0 q}{2^{2\ell}} \pmod{q}$. $\frac{p_1 q}{2^{\ell}} \in \left(-\frac{q}{2}; \frac{q}{2}\right)$, and $\frac{ab-p_0 q}{2^{2\ell}}$ is small. So $\frac{(p_1+\bar{q})q}{2^{\ell}}$ is $\frac{ab - p_0 q + q\bar{q}2^{\ell}}{2^{2\ell}} \in [0; \frac{3}{4}]$ away from what we want, because

$$-\frac{1}{2} < -\frac{q\bar{q}}{2^{\ell}} < -\frac{q\bar{q} \cdot 2^{\ell-1} + q \cdot \bar{q}2^{\ell-1}}{2^{2\ell}} < -\frac{q^2\bar{q}^2 + q2^{\ell}}{2^{2\ell}} < \frac{ab - p_0 q}{2^{2\ell}} < \frac{ab}{2^{2\ell}} < \frac{q^2\bar{q}^2}{2^{2\ell}} < \frac{1}{4}$$

Summary of Modular Reductions and multiplications

- Montgomery Reduction/Multiplication: computes a scaled result
  - 2 high and one low multiplications, when multiplications are split.
  - with a long MADD, can accumulate-then-reduce (**Kyber** point mul, **Dilithium**)
- Barrett Reduction: return final exact results, need full-length mul
- Barrett Multiplication: computes an exact result
  - 2 low and one high multiplications when multiplications are split.
  - can combine with additions or subtractions.
  - more useful for vectorized operations or the M3
- Plantard Multiplication: computes a scaled result
  - need multiply single-by-two-limbs-return-middle (**Kyber** NTT)

Here Endth the Reductions Part

Any Questions?

Original Montgomery Formulation

- Suppose we define $X^{(M)} = XR \bmod M$, so
  $a^{(M)} = aR \bmod M, b^{(M)} = bR \bmod M, c^{(M)} = cR \bmod M$, etc.
  then if we wish to compute $c = ab$, the Montgomery reduction of $a^{(M)}b^{(M)}$ is

  $$\mathrm{MM}(a^{(M)}, b^{(M)}) := \mathrm{MR}(a^{(M)}b^{(M)}) \equiv a^{(M)}b^{(M)}/R \equiv abR \equiv c^{(M)},$$

  and $a^{(M)} + b^{(M)} \equiv c^{(M)}$

Original Montgomery Formulation

- Suppose we define $X^{(M)} = XR \bmod M$, so
  $a^{(M)} = aR \bmod M, b^{(M)} = bR \bmod M, c^{(M)} = cR \bmod M$, etc.
  then if we wish to compute $c = ab$, the Montgomery reduction of $a^{(M)}b^{(M)}$ is

$$\mathrm{MM}(a^{(M)}, b^{(M)}) := \mathrm{MR}(a^{(M)}b^{(M)}) \equiv a^{(M)}b^{(M)}/R \equiv abR \equiv c^{(M)},$$

  and $a^{(M)} + b^{(M)} \equiv c^{(M)}$
- So we may make all our computations this way, we call $a^{(M)}$
  ”a in Montgomery Domain”.

Original Montgomery Formulation

- Suppose we define $X^{(M)} = XR \bmod M$, so
  $a^{(M)} = aR \bmod M, b^{(M)} = bR \bmod M, c^{(M)} = cR \bmod M$, etc.
  then if we wish to compute $c = ab$, the Montgomery reduction of $a^{(M)}b^{(M)}$ is

$$\mathrm{MM}(a^{(M)}, b^{(M)}) := \mathrm{MR}(a^{(M)}b^{(M)}) \equiv a^{(M)}b^{(M)}/R \equiv abR \equiv c^{(M)},$$

  and $a^{(M)} + b^{(M)} \equiv c^{(M)}$
- So we may make all our computations this way, we call $a^{(M)}$
  "a in Montgomery Domain".
- To compute $a^{(M)}$, compute the Montgomery reduction of $a(R^2 \bmod M)$
  (We can precompute $R^2 \bmod M$)

Montgomery Multiplication Mod an Even Number

Suppose $\gcd(M, R) \neq 1$, usually $R = 2^k$ so this means an even number (the method below can be extended if R is even more composite).

- Want ab mod M while $M \equiv 2^t u$, u is odd, $u' \equiv 1/u \bmod R, R = 2^{16}$
  $B = bR \bmod M$, so $M | (B - bR)$ hence $2^t | (B - bR)$
  $B' \equiv u' [\frac{B - bR}{2^t}] \bmod R$

Montgomery Multiplication Mod an Even Number

Suppose $\gcd(M, R) \neq 1$, usually $R = 2^k$ so this means an even number (the method below can be extended if R is even more composite).

- Want $ab \bmod M$ while $M \equiv 2^t u$, u is odd, $u' \equiv 1/u \bmod R$, $R = 2^{16}$
  $B = bR \bmod M$, so $M|(B - bR)$ hence $2^t|(B - bR)$
  $B' \equiv u'[\frac{B-bR}{2^t}] \bmod R$
- to compute $ab \bmod M$, first compute $\ell = aB' \bmod R$,
  then $ab \bmod M = (aB - \ell M)/R \bmod M$

Montgomery Multiplication Mod an Even Number

Suppose $\gcd(M, R) \neq 1$, usually $R = 2^k$ so this means an even number (the method below can be extended if R is even more composite).

- Want $ab \bmod M$ while $M \equiv 2^t u$, u is odd, $u' \equiv 1/u \bmod R$, $R = 2^{16}$
  $B = bR \bmod M$, so $M|(B - bR)$ hence $2^t|(B - bR)$
  $B' \equiv u'[\frac{B-bR}{2^t}] \bmod R$
- to compute $ab \bmod M$, first compute $\ell = aB' \bmod R$,
  then $ab \bmod M = (aB - \ell M)/R \bmod M$
  - Note: Need $aB = \ell M \pmod{R} \Leftrightarrow aB/2^t = \ell u \pmod{R/2^t}$. But this is true since $B' = u'B/2^t \pmod{R/2^t}$.

Montgomery Multiplication Mod an Even Number (cont'd)

- first, $B = bR \bmod u$, so $aB \equiv abR \pmod{u}$, $aB - \ell M \equiv abR \pmod{u}$ so $(aB - \ell M)/R \equiv ab \pmod{u}$

Montgomery Multiplication Mod an Even Number (cont'd)

- first, $B = bR \bmod u$, so $aB \equiv abR \pmod{u}$, $aB - \ell M \equiv abR \pmod{u}$ so $(aB - \ell M)/R \equiv ab \pmod{u}$
- second, we want $(aB - \ell M)/R \equiv ab \pmod{2^t}$, or $aB - \ell M \equiv abR \pmod{2^t R}$ (Reminder: $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{cm}$)

Montgomery Multiplication Mod an Even Number (cont'd)

- first, $B = bR \bmod u$, so $aB \equiv abR \pmod{u}$, $aB - \ell M \equiv abR \pmod{u}$ so $(aB - \ell M)/R \equiv ab \pmod{u}$
- second, we want $(aB - \ell M)/R \equiv ab \pmod{2^t}$, or $aB - \ell M \equiv abR \pmod{2^t R}$ (Reminder: $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{cm}$)
- since $\ell \equiv aB' \pmod{R} \Leftrightarrow \ell M \equiv aB'M \pmod{RM}$, thus $\equiv aB'M \pmod{2^t R}$ so all we need is $aB - aB'M \equiv abR \pmod{2^t R} \quad \forall a$, or $B - B'M \equiv bR \pmod{2^t R}$ or $B - bR \equiv B'M \pmod{2^t R}$

Montgomery Multiplication Mod an Even Number (cont'd)

- first, $B = bR \bmod u$, so $aB \equiv abR \pmod{u}$, $aB - \ell M \equiv abR \pmod{u}$ so $(aB - \ell M)/R \equiv ab \pmod{u}$
- second, we want $(aB - \ell M)/R \equiv ab \pmod{2^t}$, or $aB - \ell M \equiv abR \pmod{2^t R}$ (Reminder: $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{cm}$)
- since $\ell \equiv aB' \pmod{R} \Leftrightarrow \ell M \equiv aB'M \pmod{RM}$, thus $\equiv aB'M \pmod{2^t R}$ so all we need is $aB - aB'M \equiv abR \pmod{2^t R} \quad \forall a$, or $B - B'M \equiv bR \pmod{2^t R}$ or $B - bR \equiv B'M \pmod{2^t R}$
- but $B' = u' \left(\frac{B-bR}{2^t}\right) \pmod{R}$ or $\frac{BM}{2^t} \equiv uB' \equiv \left(\frac{B-bR}{2^t}\right) \pmod{R}$