Explicit Correction Probabilities for Montgomery Multiplication via Arithmetic Analysis

Daichi Aoki[1,2] Tsuyoshi Takagi[2]

[1]NEC Corporation [2]The University of Tokyo

June 30, 2026, ARITH 2026, Fulda, Germany

Motivation

Why correction probabilities matter

Modular multiplication in cryptography

- RSA: modular exponentiation.
- Lattice-based cryptography: polynomial arithmetic.
- Efficient reduction avoids costly divisions.

Common reduction methods

- Barrett reduction [Bar87].
- Montgomery reduction [Mon85].
- Plantard-style arithmetic [Pla21; AMOT22; HZZ+22].

Focus of this talk

The final conditional subtraction in Montgomery multiplication:

$$A \geq m \quad \Longrightarrow \quad A \leftarrow A - m.$$

Even when implemented branchlessly, the event itself is input-dependent and can affect timing, micro-architectural behavior, or lazy-reduction strategies.

Previous analyses and the gap

Known direction

Prior work relates Montgomery correction events to timing attacks against RSA and analyzes probabilities mainly when the modulus m is close to the Montgomery radix R [Sch00; SST04].

- Earlier estimates: about $1/3$ for squaring and $1/4$ for general multiplication when $m \approx R$ [WT01; SST04].
- Sato–Schepers–Takagi give an exact analysis in the near-radix regime [SST04].
- The small-modulus regime $m \ll R$, common in word-size arithmetic and CRT sub-moduli, is much less understood.

Question

How does the correction probability depend on the arithmetic structure of m?

Montgomery correction condition

Montgomery multiplication

Montgomery multiplication

Input: integers $R = 2^n$, odd $m < R$, and $m' = -m^{-1} \bmod R$
Input: integers x, y with $0 \le xy < mR$
Output: $A \equiv xyR^{-1} \bmod m$, $0 \le A < m$

1: $u \leftarrow xym' \bmod R$ ▷ unsigned low product
2: $A \leftarrow (xy + um)/R$ ▷ logical right shift
3: **if** $A \ge m$ **then** $A \leftarrow A - m$ ▷ correction step
4: **return** A

Before the final subtraction,

$$\widetilde{A} = \frac{xy + (xym' \bmod R)m}{R} < \frac{xy}{R} + m.$$

Thus, under $xy < mR$, at most one correction is needed.

A simpler correction condition

Standard condition

$$xy + (xym' \bmod R)m \geq mR.$$

This is correct, but the modular inverse m' makes the condition hard to count directly.

Theorem

Let $R = 2^n$ and let $m < R$ be odd. For integers $x, y \geq 0$, the correction step is performed if and only if there exists $k \geq 0$ such that

$$xy \equiv kR \pmod{m}, \qquad xy > kR.$$

Key benefit: the correction event becomes a congruence condition plus an order condition. This turns the problem into arithmetic counting.

Overview of contributions

Input model	Counting object	Main result
Modulus-size model $(x, y) \in [0, m)^2$	Pairs (x, y) satisfying for each k $\begin{cases} xy \equiv kR \pmod{m} \\ xy > kR \end{cases}$	Exact count formula; especially for $m^2 < R$, $\Pr[\text{corr}] = \dfrac{P(m) - 2m + 1}{m^2}.$
Full-size model $0 < xy \leq mR$	Divisor sums over residue classes: $\sum_{\substack{kR < n \leq mR \\ n \equiv kR \bmod m}} \tau(n)$	Exact divisor-sum representation and a heuristic main term explaining probability $\approx 1/2$ when $m \approx R$.

Here $P(m) = \sum_{j=1}^{m} \gcd(j, m)$ is the gcd-sum function and $\tau(n) = \sum_{d \mid n} 1$ is the divisor function.

Modulus-size input model

Correction sets in the modulus-size model

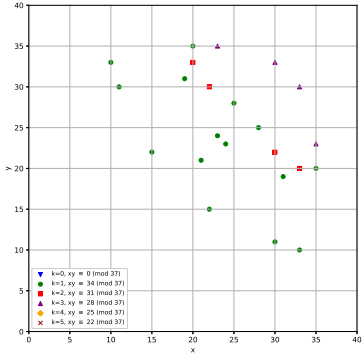
For $0 \le k < m$, define

$$S_m(k) = \left\{ (x,y) \in \mathbb{Z}^2_{\ge 0} \;\middle|\; \begin{array}{l} xy \equiv kR \bmod m, \\ xy > kR, \\ x, y < m \end{array} \right\}.$$

Then

$$S(m) = \bigcup_{k=0}^{m-1} S_m(k), \qquad \Pr[\text{corr}] = \frac{|S(m)|}{m^2}.$$

The condition $xy > kR$ cuts off a hyperbolic region; the congruence selects arithmetic patterns.



$R = 256,\ m = 37$

Correction sets in the modulus-size model

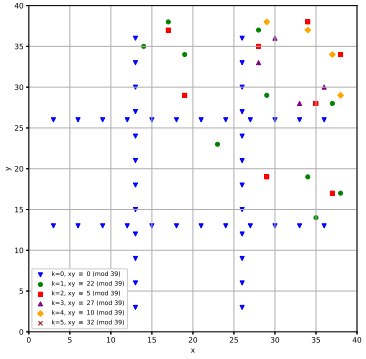
For $0 \le k < m$, define

$$S_m(k) = \left\{ (x,y) \in \mathbb{Z}^2_{\ge 0} \;\middle|\; \begin{array}{l} xy \equiv kR \bmod m, \\ xy > kR, \\ x, y < m \end{array} \right\}.$$

Then

$$S(m) = \bigcup_{k=0}^{m-1} S_m(k), \qquad \Pr[\text{corr}] = \frac{|S(m)|}{m^2}.$$

The condition $xy > kR$ cuts off a hyperbolic region; the congruence selects arithmetic patterns.



$R = 256$, $m = 39$

Exact count of $S_m(k)$

Counting theorem

If $k < m^2/R$, then

$$|S_m(k)| = \sum_{d \mid \gcd(k,m)} \sum_{\substack{kR/m < x < m \\ \gcd(x,m)=d}} \left(d - 1 - \left\lfloor \frac{kR/x - y_0(x,k)}{m/d} \right\rfloor \right),$$

where $y_0(x,k)$ is the unique solution modulo m/d of

$$(x/d)y \equiv (k/d)R \pmod{m/d}.$$

If $k \geq m^2/R$, then $|S_m(k)| = 0$.

Counting idea. Fix x and set $d = \gcd(x,m)$. The congruence $xy \equiv kR \pmod{m}$ is solvable exactly when $d \mid k$, and its solutions form $y = y_0 + j(m/d)$.

Small-modulus regime: only $k = 0$ remains

Suppose $m^2 < R$. Then $|S_m(k)| = 0$ for all $k > 0$, so only $S_m(0)$ contributes.

$$|S_m(0)| = \sum_{x=1}^{m-1} (\gcd(x, m) - 1) = P(m) - 2m + 1.$$

Therefore,

Exact probability for $m^2 < R$

$$f_0(m) = \Pr[\text{corr}] = \frac{P(m) - 2m + 1}{m^2}.$$

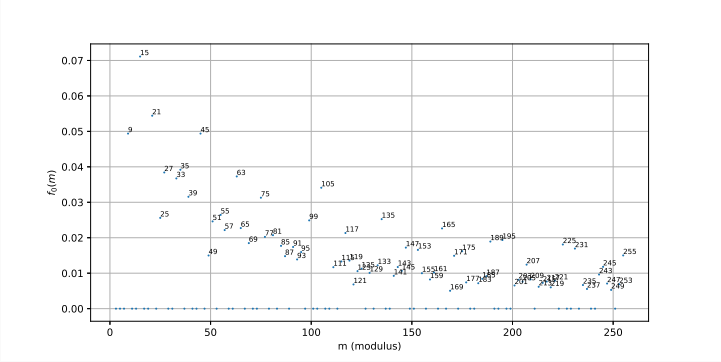
Arithmetic structure appears.

- P is multiplicative.
- For a prime power p^a,

$$P(p^a) = (a + 1)p^a - ap^{a-1}.$$

- For any prime p, $f_0(p) = 0$.

Numerical behavior of $f_0(m)$



- Odd moduli $3 \leq m < 256$.
- Zero-valued points are prime moduli.
- The largest observed value is at $m = 15$.

Empirical conjecture

For any odd $m \geq 3$,

$$f_0(m) \leq f_0(15).$$

Theoretical support for the conjecture

Prime powers

For $m = p^a$ with $p \geq 3$,

$$f_0(p^a) \leq f_0(p^2) \leq f_0(3^2) = \frac{4}{81} \approx 0.0494.$$

Products of two distinct primes

For $m = pq$ with $3 \leq p < q$,

$$f_0(pq) = \frac{2(p-1)(q-1)}{p^2q^2} \leq f_0(3 \cdot 5) = \frac{16}{225} \approx 0.0711.$$

These cases are consistent with the observed maximum at $m = 15$.

Full-size arithmetic counting model

Full-size model and exact divisor sums

Define the finite hyperbolic region

$$F_m = \{(x, y) \in \mathbb{Z}^2_{>0} \mid xy \leq mR\}.$$

Since the number of pairs with $xy = n$ is $\tau(n)$,

$$|F_m| = \sum_{n \leq mR} \tau(n).$$

Define

$$T_m(k) = \left\{ (x, y) \in \mathbb{Z}^2_{>0} \;\middle|\; \begin{array}{l} xy \equiv kR \pmod{m}, \\ kR < xy \leq mR \end{array} \right.$$

Then

$$|T_m(k)| = \sum_{\substack{kR < n \leq mR \\ n \equiv kR \bmod m}} \tau(n).$$

The correction probability is $|T(m)|/|F_m|$, where $T(m) = \bigcup_{k=0}^{m-1} T_m(k)$.

Denominator: Dirichlet's divisor-sum estimate

Dirichlet's estimate

For $X \geq 1$,

$$\sum_{n \leq X} \tau(n) = X \log X + (2\gamma - 1)X + O(\sqrt{X}),$$

where γ is Euler's constant.

Applying this with $X = mR$ gives

$$|F_m| \approx mR \log(mR) + (2\gamma - 1)mR.$$

Thus the main remaining task is to approximate the numerator $|T(m)|$.

Numerator: averaging residue-class divisor sums

For each k, put $g = \gcd(k, m)$, $k = gh$, and $m = gq$. Then

$$|T_m(k)| = \sum_{\substack{hR < N \le qR \\ N \equiv hR \bmod q}} \tau(gN).$$

Primitive residue-class average

Define

$$D_g(X; q) = \frac{1}{\varphi(q)} \sum_{\substack{N \le X \\ \gcd(N,q)=1}} \tau(gN).$$

Replace individual primitive residue classes by this average.

Using an elementary decomposition of $\tau(gN) = \sum_{d \mid \gcd(g,N)} \mu(d)\tau(g/d)\tau(N/d)$,

$$D_g(X; q) = \frac{A_{g,q}}{\varphi(q)} X \log X + O_{g,q}(X),$$

where $A_{g,q} = \left(\frac{\varphi(q)}{q}\right)^2 \sum_{\substack{d \mid \operatorname{rad}(g) \\ \gcd(d,q)=1}} \frac{\mu(d)\tau(g/d)}{d}$.

Main approximation in the full-size model

Summing over all k and using the identity

$$\sum_{q|m} qA_{m/q,q} = m,$$

the main term is

$$|T(m)| = \frac{1}{2}(m + A_{m,1})R\log R + RL(m) + E(m,R).$$

With the heuristic approximation

$$L(m) \approx \frac{1}{2}m\log m,$$

we obtain

Heuristic numerator

$$|T(m)| \approx \frac{1}{2}(m + A_{m,1})R\log R + \frac{1}{2}mR\log m.$$

Since $A_{m,1}/m \to 0$, the extra term becomes negligible for large m.

Why the probability is close to $1/2$

Combining the numerator and denominator approximations,

$$\frac{|T(m)|}{|F_m|} \approx \frac{\frac{1}{2}(m + A_{m,1})R\log R + \frac{1}{2}mR\log m}{mR\log(mR) + (2\gamma - 1)mR}.$$

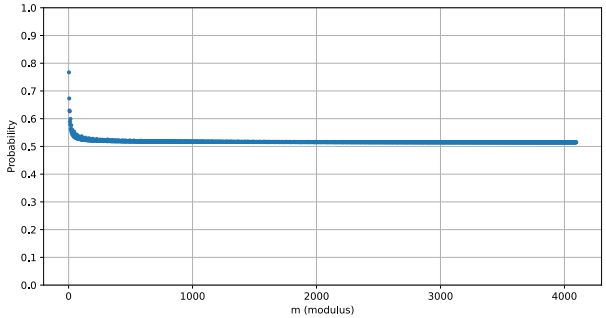
Equivalently,

$$\frac{|T(m)|}{|F_m|} \approx \frac{1}{2}\frac{\log(mR) + (A_{m,1}/m)\log R}{\log(mR) + (2\gamma - 1)}.$$

Consequence

When m is close to R and both are large, the correction probability is expected to be close to $1/2$ in this full-size arithmetic counting model.

Numerical result in the full-size model



- Exact value $|T(m)|/|F_m|$ for odd $3 \leq m < R$.
- Here $R = 4096$.
- The large-m region is consistent with the approximation $|T(m)|/|F_m| \approx 1/2$.

Conclusion

Conclusion and future work

Conclusion

- We reformulated Montgomery correction events using congruence and order constraints.
- We obtained exact formulas in the modulus-size setting, including a closed expression for $m^2 < R$.
- We derived an exact divisor-sum representation and a main-term approximation in the full-size setting.

Future work

- Prove or refine the conjectured maximum of $f_0(m)$ at $m = 15$.
- Derive a full asymptotic expansion in the modulus-size model for general m.
- Obtain uniform error terms for the full-size main-term approximation.

References

[AMOT22] D. Aoki, K. Minematsu, T. Okamura, and T. Takagi. "Efficient Word Size Modular Multiplication over Signed Integers". In: *Proc. 29th IEEE Symposium on Computer Arithmetic*. Lyon, France, 2022, pp. 94–101.

[Bar87] P. Barrett. "Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor". In: *CRYPTO'86*. Ed. by A. M. Odlyzko. Vol. 263. LNCS. Springer, Berlin, Heidelberg, 1987, pp. 311–323.

[HZZ+22] J. Huang, J. Zhang, H. Zhao, Z. Liu, R. C. C. Cheung, Ç. K. Koç, and D. Chen. "Improved Plantard Arithmetic for Lattice-based Cryptography". In: *IACR TCHES* 2022.4 (2022), pp. 614–636.

[Mon85] P. L. Montgomery. "Modular multiplication without trial division". In: *Math. Comput.* 44.170 (1985), pp. 519–521.

[Pla21] T. Plantard. "Efficient Word Size Modular Arithmetic". In: *IEEE Trans. Emerg. Top. Comput.* 9.3 (2021), pp. 1506–1518.

[Sch00] W. Schindler. “A Timing Attack against RSA with the Chinese Remainder Theorem”. In: *Proc. Cryptographic Hardware and Embedded Systems — CHES 2000*. Vol. 1965. LNCS. Worcester, MA, USA, 2000, pp. 109–124.

[SST04] H. Sato, D. Schepers, and T. Takagi. “Exact Analysis of Montgomery Multiplication”. In: *Proc. Progress in Cryptology — INDOCRYPT 2004*. Vol. 3348. LNCS. Chennai, India, 2004, pp. 290–304.

[WT01] C. D. Walter and S. Thompson. “Distinguishing Exponent Digits by Observing Modular Subtractions”. In: *Proc. Topics in Cryptology — CT-RSA 2001*. Vol. 2020. LNCS. San Francisco, CA, USA, 2001, pp. 192–207.