Modest Security Gains With Modulus Diversity in Elliptic Curve Cryptography

A. Chawla
REAL Institute
Email: editor@realinstitute.live

***Abstract*—Multi-modulus elliptic curve constructions provide only modest constant-factor security improvements, not exponential gains. Through formal analysis, we prove that distinct coprime moduli yield larger cyclic subgroups than single-modulus constructions, while identical moduli offer no asymptotic security improvement whatsoever. We examine the discrete logarithm problem in product groups and clarify common misconceptions about multi-modulus cryptographic designs. Our results show that while distinct moduli provide a structural advantage via increased subgroup order, the actual security gain is limited to a small constant-factor increase in attack complexity. This work provides rigorous bounds on the security properties of elliptic curve systems built over product rings and informs realistic expectations for cryptographic system design.**

***Index Terms*—Elliptic Curve Cryptography, Discrete Logarithm Problem, Modulus Diversity, Product Groups, Chinese Remainder Theorem**

I. Introduction

Elliptic curve cryptography (ECC) [1], [2] provides efficient public-key primitives based on the hardness of the discrete logarithm problem (DLP) in elliptic curve groups [3], [4]. A natural question arises: can we enhance security by operating over multiple elliptic curves simultaneously with different moduli[1]?

Consider a construction where a single scalar k is used across multiple curves: the public key becomes $K = (kP_1, kP_2, \ldots, kP_r)$ where each P_i is a base point on curve E over field $\mathbb{F}_{p_i}$. This can be viewed through the Chinese Remainder Theorem as operating over the product ring $\mathbb{Z}/n\mathbb{Z}$ where $n = \prod p_i$.

Two competing intuitions emerge. First, the naive view suggests that since the cyclic subgroup generated by $(P_1, \ldots, P_r)$ has order $\mathrm{lcm}(\mathrm{ord}(P_1), \ldots, \mathrm{ord}(P_r))$, the DLP should require $O(\sqrt{\mathrm{lcm}})$ operations, potentially offering significant security gains. Second, the realistic view recognizes that an attacker can solve the DLP independently in each component, requiring only $\sum_i O(\sqrt{\mathrm{ord}(P_i)})$ operations.

This paper formalizes both perspectives and establishes precise conditions under which modulus diversity provides security benefits. We prove that distinct moduli offer structural advantages but acknowledge that practical security gains are modest. Critically, we demonstrate that identical moduli with identical base points provide no security improvement whatsoever.

[1]Another possibility is multiple moduli for a single curve. See the Appendix.

II. Mathematical Framework

Let E be an elliptic curve defined by the Weierstrass equation $y^2 = x^3 + ax + b$. For distinct primes $p_1, \ldots, p_r$, we consider E over each field $\mathbb{F}_{p_i}$, obtaining groups $E(\mathbb{F}_{p_i})$.

Definition 1. For base points $P_i \in E(\mathbb{F}_{p_i})$ of order r_i, the **product construction** is the group

$$G = \langle P_1 \rangle \times \cdots \times \langle P_r \rangle$$

with base element $G_0 = (P_1, \ldots, P_r)$ and scalar multiplication defined component-wise: $k \cdot G_0 = (kP_1, \ldots, kP_r)$.

The discrete logarithm problem in G asks: given G_0 and $K = k \cdot G_0$, recover k.

III. Toy Example Construction

To ground our theoretical results, we construct a concrete example using the curve $E : y^2 = x^3 + x + 1$ over two fields:

- $\mathbb{F}_5$: yields $|E(\mathbb{F}_5)| = 9$, with base point $P_1 = (0, 1)$ of order 9
- $\mathbb{F}_{11}$: yields $|E(\mathbb{F}_{11})| = 14$, with base point $P_2 = (0, 1)$ of order 7

The product construction over $\mathbb{Z}/55\mathbb{Z}$ (via CRT) then has base point (P_1, P_2) of order $\mathrm{lcm}(9, 7) = 63$.

IV. Attack Model

We consider an adversary who observes all components of the public key and can apply standard DLP algorithms (Pollard's rho, baby-step giant-step) to each component independently. The adversary's strategy is:

1) Solve DLP in $\langle P_i \rangle$ to obtain $k \bmod r_i$ for each i
2) Apply the Chinese Remainder Theorem to reconstruct $k \bmod \mathrm{lcm}(r_1, \ldots, r_r)$

V. Results

We formalize the main lemmata.

Lemma 2 (Order of Product Base Point)**.** *Let E be an elliptic curve, and let $P_i \in E(\mathbb{F}_{p_i})$ have order r_i for $i = 1, \ldots, t$, where $p_1, \ldots, p_t$ are distinct primes. Define $G_0 = (P_1, \ldots, P_t)$ in the product group $G = \langle P_1 \rangle \times \cdots \times \langle P_t \rangle$. Then*

$$\mathit{ord}(G_0) = \mathit{lcm}(r_1, \ldots, r_t).$$

Proof: Let $\ell = \mathrm{lcm}(r_1, \ldots, r_t)$. We must show that $\ell \cdot G_0 = O$ and that no smaller positive integer m satisfies $m \cdot G_0 = O$.

First, observe that $\ell \cdot G_0 = (\ell P_1, \ldots, \ell P_t)$. Since $r_i \mid \ell$ for all i, we have $\ell P_i = O$ for each component, hence $\ell \cdot G_0 = O$.

Conversely, suppose $m \cdot G_0 = O$ for some $m < \ell$. Then $mP_i = O$ for all i, which implies $r_i \mid m$ for all i. Therefore $\mathrm{lcm}(r_1, \ldots, r_t) \mid m$, contradicting $m < \ell$. ■

Corollary 3 (Security Implication)**.** *When* $\gcd(r_i, r_j) = 1$ *for all* $i \neq j$*, the order is* $ord(G_0) = \prod_{i=1}^{t} r_i$*, which exceeds* $\max\{r_1, \ldots, r_t\}$ *by a factor of at least* $\min\{r_i : i \neq \arg\max r_j\}$.

This establishes that distinct moduli create a larger key space than any single component. However, this does not immediately translate to proportional security gains, as the next result clarifies.

Lemma 4 (Degeneracy of Identical Moduli)**.** *Let* $E(\mathbb{F}_p)$ *be an elliptic curve group and* $P \in E(\mathbb{F}_p)$ *a point of order* r*. Consider the product construction*

$$H = \langle P \rangle \times \langle P \rangle \subset E(\mathbb{F}_p) \times E(\mathbb{F}_p)$$

with base point $H_0 = (P, P)$ *and scalar multiplication* $k \cdot H_0 = (kP, kP)$*. Then:*

1) *ord*$(H_0) = r$ *(not* r^2*)*
2) *The DLP in* H *is no harder than the DLP in* $\langle P \rangle$

Proof: (1) By Lemma 1, $\mathrm{ord}(H_0) = \mathrm{lcm}(r, r) = r$.

(2) Given $K = (kP, kP)$, an adversary computes the discrete logarithm of the first component to obtain $k' \in \{0, \ldots, r-1\}$ such that $k'P$ equals the first coordinate. Since both coordinates are identical and equal kP, we have $k' = k \bmod r$, which completely determines k in the key space $\mathbb{Z}/r\mathbb{Z}$.

The second component provides no additional information or security. The computational cost is $O(\sqrt{r})$, identical to solving DLP in a single group $\langle P \rangle$. ■

A. Concrete Comparison

Returning to our toy example with $E : y^2 = x^3 + x + 1$:

Distinct moduli case ($p_1 = 5$, $p_2 = 11$): The base point (P_1, P_2) has order 63. A naive analysis suggests $O(\sqrt{63}) \approx 7.9$ operations. However, an adversary solves two independent DLPs requiring $O(\sqrt{9}) + O(\sqrt{7}) \approx 3 + 2.6 = 5.6$ operations, then combines results via CRT. This is approximately 1.9 times harder than attacking a single component.

Identical moduli case ($p_1 = p_2 = 5$): The base point (P_1, P_1) has order 9. The adversary needs only $O(\sqrt{9}) = 3$ operations, gaining no advantage over single-curve ECC.

VI. Discussion

Our results establish a nuanced picture of security gains from modulus diversity in elliptic curve cryptography. Lemma 1 proves that distinct coprime moduli provide a genuine structural advantage: the cyclic subgroup order increases to the least common multiple of component orders, expanding the key space. However, Lemma 3 demonstrates that identical moduli with identical base points offer zero asymptotic security improvement.

TABLE I

Security gains from modulus diversity remain modest even as component count increases. A single 256-bit curve combined with t distinct moduli yields only $256 + \log_2(t)$ bits of security, not $256t$ bits.

Components (t)	**Single curve**	**Multi-modulus**	**Gain**
1	256 bits	256 bits	0 bits
2	256 bits	257 bits	1 bit
4	256 bits	258 bits	2 bits
8	256 bits	259 bits	3 bits
16	256 bits	260 bits	4 bits
32	256 bits	261 bits	5 bits
64	256 bits	262 bits	6 bits
128	256 bits	263 bits	7 bits

The critical insight lies in the gap between structural properties and attack complexity. While distinct moduli create a larger group, realistic attackers exploit the product structure by solving component DLPs independently. The total work is approximately $\sum_i O(\sqrt{r_i})$ rather than $O(\sqrt{\prod r_i})$ or $O(\sqrt{\mathrm{lcm}(r_i)})$.

For components of roughly equal size r, this yields security of $O(t\sqrt{r})$ where t is the number of components, compared to $O(\sqrt{r})$ for a single component. In terms of bit security, if a single curve provides b bits of security, the multi-modulus construction provides approximately $b + \log_2(t)$ bits—a modest additive improvement, not a multiplicative one (see also Table I).

This has important implications for cryptographic system design [5], [6]. Practitioners should not expect that combining two 256-bit curves yields 512-bit security. Instead, the gain is closer to 256 + $\log_2(2)$ = 257 bits. The overhead of managing multiple moduli, implementing CRT operations, and handling larger key representations may outweigh this marginal security increase.

Our work also clarifies a common misconception: simply duplicating components (identical moduli, identical points) provides no benefit and only increases computational and storage costs. Any multi-modulus construction must use genuinely distinct moduli to achieve even modest gains.

Future work should investigate whether carefully chosen moduli with specific mathematical relationships could provide superadditive security gains, though current understanding suggests this is unlikely for standard DLP-based constructions. Additionally, formal security proofs [7], [8] in specific cryptographic protocols (key exchange, signatures) using multi-modulus constructions warrant investigation.

VII. Conclusion

We have formalized the security properties of multi-modulus elliptic curve constructions, proving that distinct moduli offer structural advantages while identical moduli offer none. The key takeaway is honest advertising: modulus diversity provides measurable but modest security improvements - a small constant factor in attack complexity, not exponential gains. Cryptographic designs should weigh these marginal benefits against implementation complexity and performance costs.

Acknowledgments

This work was produced with the assistance of language models.

Appendix

The main text analyzes the product group construction $E(\mathbb{F}_{p_1}) \times E(\mathbb{F}_{p_2}) \times \cdots$, which can be viewed as multiple curve groups combined. This appendix examines the mathematically equivalent but conceptually distinct perspective: working with a single curve defined directly over a product ring $\mathbb{Z}/n\mathbb{Z}$ where $n = \prod p_i$. As noted in the introduction, this represents an alternative framing of modulus diversity.

A. The Ring-Theoretic Perspective

Rather than explicitly working with pairs of points from separate groups, we can define the curve equation with coefficients in the ring $\mathbb{Z}/n\mathbb{Z}$ itself. For concreteness, consider $n = 55 = 5 \times 11$ and the Weierstrass equation:

$$E : y^2 = x^3 + x + 1 \quad \text{over } \mathbb{Z}/55\mathbb{Z}.$$

Here, $x, y \in \mathbb{Z}/55\mathbb{Z}$ and all arithmetic (addition, multiplication) happens in this ring. A cryptographic key might be a point $P = (x, y)$ where $x = 17 \in \mathbb{Z}/55\mathbb{Z}$ and $y = 23 \in \mathbb{Z}/55\mathbb{Z}$.

By the Chinese Remainder Theorem, since $\gcd(5, 11) = 1$, we have the ring isomorphism:

$$\mathbb{Z}/55\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}.$$

This isomorphism extends to curves:

$$E(\mathbb{Z}/55\mathbb{Z}) \cong E(\mathbb{Z}/5\mathbb{Z}) \times E(\mathbb{Z}/11\mathbb{Z}).$$

Since 5 and 11 are prime, $\mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$ and $\mathbb{Z}/11\mathbb{Z} = \mathbb{F}_{11}$ are fields, giving:

$$E(\mathbb{Z}/55\mathbb{Z}) \cong E(\mathbb{F}_5) \times E(\mathbb{F}_{11}).$$

B. Conceptual Distinction

The key distinction is one of representation and implementation:

- **Main text approach**: Explicitly maintain separate points $P_1 \in E(\mathbb{F}_5)$ and $P_2 \in E(\mathbb{F}_{11})$, perform operations in each group independently, then combine results. This is the "product group" view.
- **Appendix approach**: Store a single point $P = (x, y)$ with $x, y \in \mathbb{Z}/55\mathbb{Z}$, perform arithmetic modulo 55, letting the ring structure implicitly handle the factorization. This is the "single curve over a ring" view.

Under the hood, via CRT, both approaches perform identical computations. A point $(17, 23) \in \mathbb{Z}/55\mathbb{Z} \times \mathbb{Z}/55\mathbb{Z}$ corresponds to the pair $((17 \bmod 5, 23 \bmod 5), (17 \bmod 11, 23 \bmod 11)) = ((2, 3), (6, 1))$ in $\mathbb{F}_5 \times \mathbb{F}_{11}$.

C. Why ECC Works Over Product Rings

Elliptic curve cryptography typically requires working over fields to ensure well-defined group operations (specifically, to guarantee inverses exist for the point addition formulas). However, when the ring is a product of fields via CRT—as is the case with $\mathbb{Z}/n\mathbb{Z}$ where $n = \prod p_i$ for distinct primes p_i—the curve and its group structure decompose cleanly.

Critically, the product ring $\mathbb{Z}/55\mathbb{Z}$ is *not* a field (it has zero divisors), but the CRT isomorphism allows us to:

1) Define points over $\mathbb{Z}/55\mathbb{Z}$ via the isomorphism to $\mathbb{F}_5 \times \mathbb{F}_{11}$
2) Perform group operations component-wise in each field (where standard ECC applies)
3) Represent results as elements of $\mathbb{Z}/55\mathbb{Z}$ via CRT

All actual elliptic curve arithmetic happens in the field components where the standard group law is well-defined. The ring structure provides a compact encoding via CRT.

D. ECC Over General Rings

It is actually possible to define elliptic curve group laws over more general rings, including rings with zero divisors like $\mathbb{Z}/25\mathbb{Z}$ (where $25 = 5^2$), provided the curve remains non-singular modulo the relevant primes. ECC over such rings is feasible from a mathematical standpoint.

For the curve $E : y^2 = x^3 + x + 1$ over $\mathbb{Z}/25\mathbb{Z}$, we must check that the discriminant $\Delta = -16(4a^3 + 27b^2) = -16(4 + 27) = -496$ is not divisible by 5 (the prime underlying 25). Computing: $-496 \equiv 4 \pmod 5 \not\equiv 0$, so the curve is non-singular modulo 5, and a group law can be defined.

The point set over $\mathbb{Z}/25\mathbb{Z}$ forms a group where addition is well-defined for all pairs of points (with appropriate handling of special cases). One can perform scalar multiplication, generate base points, and define discrete logarithm problems—all the operations needed for cryptographic protocols.

E. Why Prime Powers Offer No Cryptographic Advantage

While ECC over $\mathbb{Z}/p^k\mathbb{Z}$ is mathematically feasible, it provides no security benefit for cryptography. The critical issue is that the DLP over $\mathbb{Z}/p^k\mathbb{Z}$ reduces efficiently to the DLP over $\mathbb{F}_p$:

1) An attacker solves the discrete logarithm modulo p (the hardest step)
2) The solution modulo p can be lifted to a solution modulo p^k using Hensel's lemma or similar techniques with only polynomial overhead

Therefore, the security of ECC over $\mathbb{Z}/25\mathbb{Z}$ is essentially equivalent to the security over $\mathbb{F}_5$, despite the larger ring. The additional structure provided by p^k does not increase the computational difficulty for an adversary.

This explains why our construction uses $n = 55 = 5 \times 11$ (distinct primes) rather than $n = 25 = 5^2$ (prime power). The product of distinct primes via CRT gives genuine security benefits: an attacker must solve independent DLPs in each prime field component. Prime powers, while mathematically workable, add implementation complexity without cryptographic gain.

F. Equivalence of Security Gains

The single-curve-over-product-ring construction in this appendix yields *identical* security properties to the product-group construction in the main text. This is because they are mathematically the same construction via CRT—merely represented differently.

From Section III of the main text, we have $\langle P_1 \rangle$ of order 9 in $E(\mathbb{F}_5)$ and $\langle P_2 \rangle$ of order 7 in $E(\mathbb{F}_{11})$. The product group has order $\text{lcm}(9, 7) = 63$. In the ring perspective, a base point in $E(\mathbb{Z}/55\mathbb{Z})$ corresponds to this same pair under CRT, giving order 63.

In both cases, an adversary faces identical attack complexity:

- Solve DLP in the mod-5 component: $O(\sqrt{9}) = 3$ operations
- Solve DLP in the mod-11 component: $O(\sqrt{7}) \approx 2.6$ operations
- Combine via CRT: negligible overhead
- **Total**: $O(\sqrt{9}) + O(\sqrt{7}) \approx 5.6$ operations

This is approximately 1.9 times harder than attacking a single component, matching the concrete comparison in the Results section (Section V) of the main text.

The "modest" improvement is identical because whether we:

1) Store and manipulate points as elements of $\mathbb{Z}/55\mathbb{Z}$ (ring view), or
2) Explicitly work with pairs from $E(\mathbb{F}_5) \times E(\mathbb{F}_{11})$ (product view)

makes no difference to the adversary's task.

The equivalence arises from the Chinese Remainder Theorem, which establishes that working with numbers modulo 55 is the same as working with pairs of numbers modulo 5 and modulo 11 simultaneously. Every point (x, y) with coordinates in $\mathbb{Z}/55\mathbb{Z}$ uniquely corresponds to a pair of points—one with coordinates in $\mathbb{Z}/5\mathbb{Z}$ and one with coordinates in $\mathbb{Z}/11\mathbb{Z}$. The CRT provides a dictionary for translating between these two views: the single-ring perspective treats everything as operations modulo 55, while the product perspective explicitly tracks the two components separately, but they describe identical mathematical objects and operations.

The security gain remains a constant factor of approximately 1.9, not an exponential improvement.

For practical cryptography with standardized curves (e.g., combining two 256-bit curves), both approaches yield the same modest gain of approximately 1 additional bit of security (cf. Table I), while requiring management of multiple moduli and CRT operations.

References

[1] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[2] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO'85*, ser. Lecture Notes in Computer Science, vol. 218. Springer, 1986, pp. 417–426.

[3] J. M. Pollard, "Monte Carlo methods for index computation (mod *p*)," *Mathematics of Computation*, vol. 32, no. 143, pp. 918–924, 1978.

[4] D. Shanks, "Class number, a theory of factorization, and genera," in *Proceedings of Symposia in Pure Mathematics*, vol. 20, 1971, pp. 415–440.

[5] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Springer, 2004.

[6] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, 2nd ed. Chapman and Hall/CRC, 2008.

[7] M. Bellare, R. Canetti, and H. Krawczyk, "A modular approach to the design and analysis of authentication and key exchange protocols," in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC'98)*, 1998, pp. 419–428.

[8] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. Chapman and Hall/CRC, 2014.