Casting out Primes: Bignum Arithmetic for Zero-Knowledge Proofs

Daniel Lubarov
daniel.l@polygon.technology

Jordi Baylina
jordi@polygon.technology

October 26, 2022

Abstract

We describe a nondeterministic method for bignum arithmetic. It is inspired by the "casting out nines" technique, where some identity is checked modulo 9, providing a probabilistic result.

More generally, we might check that some identity holds under a set of moduli, i.e. $f(\vec{x}) = 0 \mod m_i$ for each $m_i \in M$. Then $f(\vec{x}) = 0 \mod \operatorname{lcm}(M)$, and if we know $|f(\vec{x})| < \operatorname{lcm}(M)$, it follows that $f(\vec{x}) = 0$.

We show how to perform such small-modulus checks efficiently, for certain $f(\vec{x})$ such as bignum multiplication. We focus on the cost model of zero-knowledge proof systems, which support field arithmetic and range checks as native operations.

Contents

1 Preliminaries

Let $[b]$ denote the set $\{0, \ldots, b-1\}$. A bignum consisting of n limbs in base b can be represented by a tuple in $[b]^n$.

There exists a canonical isomorphism between $[b]^n$ and $[b^n]$, that is, between a tuple of limbs and the integer they encode. Its forward map $[b]^n \to [b^n]$ is simply

$$\sigma_b(x) = \sum_{i=0}^{n-1} b^i x_i.$$

Given a pair of bignums, $x, y \in [b]^n$, the product $\sigma_b(x)\sigma_b(y)$ can be written as a function $([b]^n, [b]^n) \to [b^{2n}]$, namely

$$\pi_b(x, y) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} b^{i+j} x_i y_i.$$

1.1 Partially reduced summations

When checking an identity mod m, it can be useful to *partially* reduce $\sigma_b(x)$ mod m by reducing each b^i expression. Let

$$\sigma_b^{(m)}(x) = \sum_{i=0}^{n-1} (b^i \bmod m) x_i.$$

Similarly, we can partially reduce $\pi_b(x, y)$ mod m as

$$\pi_b^{(m)}(x, y) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (b^{i+j} \bmod m) x_i y_i.$$

Note that $\sigma_b(x) = \sigma_b^{(m)}(x) \mod m$, and likewise $\pi_b(x, y) = \pi_b^{(m)}(x, y) \mod m$.

From the summations above, one can trivially deduce the following bounds:

Theorem 1. *Given $x \in [b]^n$, $\sigma_b^{(m)}(x) < nmb$. Given $x, y \in [b]^n$, $\pi_b^{(m)}(x, y) < n^2 mb^2$.*

1.2 Notation

Given $x \in [b]^n$, we sometimes use x and $\sigma_b(x)$ interchangeably when the meaning is clear from context. For example, $x < b^n$ is shorthand for $\sigma_b(x) < b^n$.

2 Widening multiplication

We first consider the problem of multiplying two bignums, $x, y \in [b]^n$. Instead of computing xy deterministically, we will witness their product $z \in [b]^{2n}$, then check that $xy = z$.

Rather than verifying this identity directly, we will check that it holds under a set of moduli, $M = \{m_0, \ldots, m_{k-1}\}$. Suppose that for each m_i, $xy = z \mod m_i$, or equivalently, $m_i \mid (xy - z)$. Then $\mathrm{lcm}(M) \mid (xy - z)$, where lcm denotes the least common multiple function.

Since $xy < b^{2n}$ and $z < b^{2n}$, $|xy - z| < b^{2n}$. If we select M such that $\mathrm{lcm}(M) \geq b^{2n}$, then $|xy - z| < \mathrm{lcm}(M)$, so $xy - z = 0$ is the only solution to $\mathrm{lcm}(M) \mid (xy - z)$. Hence, $xy = z$.

Remark 1. *Pairwise coprime sets are natural choices for M, since they have the property that* $\mathrm{lcm}(M) = \prod_{i=0}^{k-1} m_i$.

2.1 Congruence mod m_i

It remains to check $xy = z \mod m_i$, or more precisely, $\pi_b(x, y) = \sigma_b(z) \mod m_i$. By partially reducing both sides, we can reduce the problem to

$$\pi_b^{(m_i)}(x, y) = \sigma_b^{(m_i)}(z) \mod m_i.$$

Rather than deterministically reducing both sides, we can witness $s \in \mathbb{Z}$ such that

$$\pi_b^{(m_i)}(x, y) - \sigma_b^{(m_i)}(z) = s m_i. \tag{1}$$

The following bound on $|s|$ trivially follows from Theorem 1:

Theorem 2. *If s is a valid solution to Equation 1, $|s| < n^2 b^2$.*

2.2 Avoiding wrap-around

With a computation model based on prime field arithmetic, we cannot check Equation 1 directly. We can only check that it holds mod p, or equivalently, that there exists some t such that

$$\pi_b^{(m_i)}(x, y) - \sigma_b^{(m_i)}(z) - s m_i = tp.$$

To prevent invalid solutions involving wrap-around, we must bound the left-hand side such that $t = 0$ is the only possible solution. In particular, we must ensure that

$$\left| \pi_b^{(m_i)}(x, y) - \sigma_b^{(m_i)}(z) - s m_i \right| < p.$$

Applying the triangle inequality, and leveraging the fact that $\pi_b^{(m_i)}(x, y)$ and $-\sigma_b^{(m_i)}(z)$ have opposite signs, it suffices to ensure that

$$\max\left\{\pi_b^{(m_i)}(x, y), \sigma_b^{(m_i)}(z)\right\} + |sm_i| < p,$$

or, applying Theorem 1 and Theorem 2, that

$$2n^2 m_i b^2 \leq p.$$

We will pick a set of parameters for which this holds.

Remark 2. *It is natural to include p itself in M, since we can check an identity mod p "natively." Clearly p itself need not satisfy the bound above, since wrap-around is not an issue when we are checking an identity mod p.*

3 Modular multiplication

Suppose we wish to compute modular multiplication with a fixed modulus, $q < b^n$. As before, we are given $x, y \in [b]^n$ as inputs, and we will witness $z \in [b]^n$. But instead of checking $xy = z$, our goal now is to check $xy = z \mod q$.[1]

To do so, we could witness r such that $\pi_b(x, y) - \sigma_b(z) = rq$. However, we can reduce the problem size by instead witnessing r such that $\pi_b^{(q)}(x, y) - \sigma_b^{(q)}(z) = rq$. Theorem 1 then implies $|r| < n^2 b^2$, which we would enforce with a range check.

As before, we test this under a set of moduli M. From Theorem 1 and the triangle inequality, we know

$$\left|\pi_b^{(q)}(x, y) - \sigma_b^{(q)}(z) - rq\right| < 2n^2 q b^2,$$

so we select M such that $\text{lcm}(M) \geq 2n^2 q b^2$. Note that we would have needed a larger $\text{lcm}(M)$ had we not performed the partial reduction mod q.

3.1 Congruence mod m_i

Our small-moduli checks now have the form

$$\pi_b^{(q)}(x, y) - \sigma_b^{(q)}(z) = rq \mod m_i.$$

Applying partial reductions mod m_i to all constants, we have

$$\pi_b^{(q)(m_i)}(x, y) - \sigma_b^{(q)(m_i)}(z) = r(q \bmod m_i) \mod m_i,$$

[1] To ensure that the result is in the canonical range $[q]$, we would need to additionally enforce $z < q$. In practice, however, a partial reduction to $[b^n]$ suffices for most applications.

where $(q)(m_i)$ denotes a sequence of partial reductions, i.e.,

$$\sigma_b^{(q)(m_i)} = \sum_{i=0}^{n-1} ((b^i \bmod q) \bmod m_i) x_i,$$

and similarly for $\pi_b^{(q)(m_i)}(x, y)$.

Now, we witness s such that

$$\pi_b^{(q)(m_i)}(x, y) - \sigma_b^{(q)(m_i)}(z) - r(q \bmod m_i) = s m_i.$$

Theorem 1 implies $|s| < 2n^2 b^2$, which we enforce with a range check.

3.2 Avoiding wrap-around

Finally, as in Section 2.2, we must choose our parameters such that wrap-around is not possible when the constraint above is checked mod p. Using a similar analysis, it suffices that

$$4n^2 m_i b^2 \leq p.$$

3.3 Example parameters

Suppose our "native" field is $\mathbb{F}_p$ where $p = 2^{64} - 2^{32} + 1$. Suppose we would like to perform multiplication over the secp256k1 base field, $\mathbb{F}_q$, where $q = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$. Let $n = 16$ and $b = 2^{16}$.

To avoid wrap-around, we require each m_i (except for p itself, as noted in Remark 2) to satisfy

$$m_i \leq \frac{p}{4n^2 b^2},$$

which (after rounding down) is 4194303, or roughly 2^{22}.

Additionally, M must satisfy $\mathrm{lcm}(M) \geq 2n^2 q b^2$, which is roughly 2^{297}. One such M is

$$\begin{aligned} M = (&p, 4194272, 4194273, 4194275, 4194277, 4194281, 4194283,\\ &4194287, 4194289, 4194293, 4194299, 4194301), \end{aligned}$$

a pairwise coprime set which satisfies both of these constraints.

4 Probabilistic method

Instead of fixing M, we can sample it as a random subset of some larger pairwise coprime set $\mathbb{M}$. Given our bound $|xy - z| < b^{2n}$, we can argue that only a small fraction of $\mathbb{M}$ can divide $xy - z$, so if $xy \neq z$, the identity is unlikely to hold under all $m \in M$. Depending on our security parameter, this may enable us to use a smaller M relative to the previous method.

4.1 Example parameters

Concretely, let $\mathbb{M}$ be a pairwise coprime subset of $[2^{15}, .., 2^{16}]$. We found such a set containing 3082 integers.

If xy and z both fit within 512 bits, $xy - z$ can be divisible by at most 34 $m_i \in \mathbb{M}$; any subset of size 35 or more would have a product exceeding 2^{512}. Thus if $xy \neq z$, the probability that $xy = z \mod m_i$ given a random $m_i \in \mathbb{M}$ is at most 34/3069.

If we sample each $m_i \in \mathbb{M}$ independently, in which case duplicates are possible, then 20 samples provides 128-bit security: $(34/3069)^{20} < 2^{-128}$. If our sampling process prevents duplicates, then 19 samples suffices, since

$$\prod_{i=0}^{18} \left(\frac{34 - i}{3069 - i} \right) < 2^{-128}.$$