A function to calculate all relative prime numbers up to the product of the first n primes

Matthias Schmitt*

May 23, 2014

Abstract

We prove an isomorphism between the finite domain $F_{\prod p_i}$ and the new defined set of prime modular numbers. This definition provides some insights about relative prime numbers. We provide an inverse function from the prime modular numbers into $F_{\prod p_i}$. With this function we can calculate all numbers from 1 up to the product of the first n primes that are not divisible by the first n primes. This function provides a non sequential way for the calculation of prime numbers.

1 prime modular numbers

Definition: Let $n \in \mathbb{N}$ and $p_i, i = 1..n$ the first n prime numbers. The prime modular numbers of level n are tuples of length n defined by

$$PM(n) := \left\{ \begin{pmatrix} t_1 & \text{mod} & 2 \\ t_2 & \text{mod} & 3 \\ t_3 & \text{mod} & 5 \\ t_4 & \text{mod} & 7 \\ \vdots \\ t_n & \text{mod} & p_n \end{pmatrix} \mid t_i \in \mathbb{N} \right\}.$$ 

The set of all prime modular numbers of length n is called $PM(n)$.

Example: For level n=1 there are two prime modular numbers:

$PM(1) = \{(0), (1)\}$

For level n=2 there are six prime modular numbers:

$PM(2) = \{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \}$

*mschmitt@db12.de, diploma mathematician graduated in Mathematical Institute, University of Cologne, 1997
Definition: The primorial number $\prod_{i=1}^{n} p_i$ is defined as the product of the first $n$ prime numbers.

Lemma 1.1 The number of elements in $PM(n)$ equals the primorial number $\prod_{i=1}^{n} p_i$.

Proof: The number of different elements on position $i \in \{1, \ldots, n\}$ equals $p_i$ due to the definition of the mod() function. The number of permutations of the first $n$ primes equals $\prod_{i=1}^{n} p_i$.

2 Isomorphism $f : F_{\prod p_i} \to PM(n)$

Definition: We define addition in $PM(n)$ by:

$$
\begin{pmatrix}
    s_1 \mod 2 \\
    s_2 \mod 3 \\
    s_3 \mod 5 \\
    \vdots \\
    s_n \mod p_n
\end{pmatrix}
+ 
\begin{pmatrix}
    t_1 \mod 2 \\
    t_2 \mod 3 \\
    t_3 \mod 5 \\
    \vdots \\
    t_n \mod p_n
\end{pmatrix}
= 
\begin{pmatrix}
    (s_1 + t_1) \mod 2 \\
    (s_2 + t_2) \mod 3 \\
    (s_3 + t_3) \mod 5 \\
    \vdots \\
    (s_n + t_n) \mod p_n
\end{pmatrix}.
$$

Definition: We define multiplication in $PM(n)$ by:

$$
\begin{pmatrix}
    s_1 \mod 2 \\
    s_2 \mod 3 \\
    s_3 \mod 5 \\
    \vdots \\
    s_n \mod p_n
\end{pmatrix}
\ast 
\begin{pmatrix}
    t_1 \mod 2 \\
    t_2 \mod 3 \\
    t_3 \mod 5 \\
    \vdots \\
    t_n \mod p_n
\end{pmatrix}
= 
\begin{pmatrix}
    (s_1 \ast t_1) \mod 2 \\
    (s_2 \ast t_2) \mod 3 \\
    (s_3 \ast t_3) \mod 5 \\
    \vdots \\
    (s_n \ast t_n) \mod p_n
\end{pmatrix}.
$$

Definition: Let be $F_{\prod p_i} = \{1, 2, \ldots, \prod_{i=1}^{n} p_i\}$. $F_{\prod p_i}$ is a finite integral domain of size $\prod_{i=1}^{n} p_i$.

We define the homomorphism $f : F_{\prod p_i} \to PM(n)$:

$$
f(k) := 
\begin{pmatrix}
    k \mod 2 \\
    k \mod 3 \\
    k \mod 5 \\
    \vdots \\
    k \mod p_n
\end{pmatrix}.
$$
Proposition 1 (Isomorphism from $F_{\prod p_i}$ into $\text{PM}(n)$) Let $k \in F_{\prod p_i}$ and $f$ the homomorphism:

$$f(k) := \begin{pmatrix} k \mod 2 \\ k \mod 3 \\ k \mod 5 \\ \vdots \\ k \mod p_n \end{pmatrix} \in \text{PM}(n)$$

$f$ is an isomorphism.

**Proof:** To prove the isomorphism, we show that $f(m + n) = f(m) + f(n)$, $f(m \ast n) = f(m) \ast f(n)$ and $f$ is injective.

a) $f(m + n) = \begin{pmatrix} m + n \mod 2 \\ m + n \mod 3 \\ m + n \mod 5 \\ \vdots \\ m + n \mod p_n \end{pmatrix} = \begin{pmatrix} m \mod 2 + n \mod 2 \\ m \mod 3 + n \mod 3 \\ m \mod 5 + n \mod 5 \\ \vdots \\ m \mod p_n + n \mod p_n \end{pmatrix} = f(m) + f(n)$

b) $f(m \ast n) = \begin{pmatrix} m \ast n \mod 2 \\ m \ast n \mod 3 \\ m \ast n \mod 5 \\ \vdots \\ m \ast n \mod p_n \end{pmatrix} = \begin{pmatrix} m \mod 2 \ast n \mod 2 \\ m \mod 3 \ast n \mod 3 \\ m \mod 5 \ast n \mod 5 \\ \vdots \\ m \mod p_n \ast n \mod p_n \end{pmatrix} = f(m) \ast f(n)$

c) $f$ is injective:

$$f(1) = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \quad \text{and} \quad f(\prod p_i) = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$
Due to This is impossible, therefore f is injective.

Thus

\[ \forall m, n \in \mathbb{Z}_p^n : f(m) = f(n) \Rightarrow f(m + 1) = f(n + 1) \]

Thus

\[ \forall m, n, r \in \mathbb{Z}_p^n : f(m) = f(n) \Rightarrow f(m + r) = f(n + r) \ [\alpha] \]

Suppose there are two values

\[ m, n \in \mathbb{Z}_p^n \text{ and } n > m \text{ with } f(m) = f(n) \]

Then there is

\[ r := \prod p_i - n \text{ and } f(n + r) = f(\prod p_i) = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \]

Due to [\alpha]:

\[ f(n + r) = f(m + r) = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \]

So there must be an value \( m < \prod p_i \) that is divisible by the first \( n \) primes.
This is impossible, therefore \( f \) is injective. \[ \Box \]

**Example:** For level n=2:

| \( k \) | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| \( f(k) \) | \begin{pmatrix} 1 \\ 1 \\ 0 \\ 2 \end{pmatrix} | \begin{pmatrix} 0 \\ 2 \\ 3 \\ 0 \end{pmatrix} | \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} | \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix} | \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} |

For level n=3:

\[ f(1) = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, f(2) = \begin{pmatrix} 0 \\ 2 \\ 2 \end{pmatrix}, f(3) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 3 \end{pmatrix}, f(4) = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 4 \end{pmatrix}, f(5) = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \end{pmatrix}, f(6) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \]

\[ f(7) = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, f(8) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 4 \end{pmatrix}, f(9) = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, f(10) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, f(11) = \begin{pmatrix} 1 \\ 2 \\ 1 \\ 2 \end{pmatrix}, f(12) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 2 \end{pmatrix}, f(13) = \begin{pmatrix} 1 \\ 3 \\ 1 \\ 3 \end{pmatrix}, f(14) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 2 \\ 4 \end{pmatrix}, f(15) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, f(16) = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, f(17) = \begin{pmatrix} 1 \\ 2 \\ 2 \\ 2 \end{pmatrix}, f(18) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 2 \\ 3 \end{pmatrix}, \]

4
\[ f(19) = \begin{pmatrix} 1 \\ 1 \\ 4 \end{pmatrix}, f(20) = \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}, f(21) = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, f(22) = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, f(23) = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, f(24) = \begin{pmatrix} 0 \\ 0 \\ 4 \end{pmatrix}, \]

\[ f(25) = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, f(26) = \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}, f(27) = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, f(28) = \begin{pmatrix} 1 \\ 1 \\ 3 \end{pmatrix}, f(29) = \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix}, f(30) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \]

**Corollary 1** \( PM(n) \) is a finite integral domain of size \( \prod_{i=1}^{n} p_i \).

**Remark:** The main drawback for calculation with prime modular numbers, is that it is no longer possible to compare two numbers and decide which one is bigger. But we get some other advantages instead, because it is much easier to decide whether a number is relative prime.

There is an inverse function \( f^{-1} : PM(n) \to F_{\prod p_i} \) that will be discussed in chapter 4.

## 3 relative prime elements

**Definition:** Given the set \( PM(n) \). An element in \( PM(n) \) is said to be **relative prime** if it has no zeros in its tuple.

**Lemma 3.1** The size of the set \( PM(n) \) is \( \prod_{i=1}^{n} (p_i - 1) \).

**Proof:** The number of values in a prime modular number on each position without 0 is \( p_i - 1 \). Therefore the number of possible permutations is \( \prod_{i=1}^{n} (p_i - 1) \).

**Example:** in \( PM(3) \) there are 8 relative prime elements:

\[
1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, 7 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, 13 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, 19 = \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \\
11 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, 17 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}, 23 = \begin{pmatrix} 2 \\ 3 \end{pmatrix}, 29 = \begin{pmatrix} 2 \\ 4 \end{pmatrix}.
\]

**Definition:** Given the set \( PM(n) \) and the isomorphism \( f : F_{\prod p_i} \to PM(n) \). We define \( f^{-1} : PM(n) \to F_{\prod p_i} \) as the **inverse function** to \( f \) with

\[
\forall k \in F_{\prod p_i} : f^{-1}(f(k)) = k
\].

5
**Definition:** Given the set $PM(n)$. We define the prime elements
t $t \in PM(n)$ as all elements, with $f^{-1}\left(\begin{array}{c} t_1 \\ t_2 \\ \vdots \\ t_{p_n} \end{array}\right)$ is prime in $F_{\prod p_i}$.

**Lemma 3.2** Let $p_{n+1}$ be the $(n+1)$-th prime number in $N$.
Let $Q = \{q \text{ is prime } \land p_{n+1} \leq q < \prod_{i=1}^{n} p_i \}$. 
\forall q \in Q : f(q) \text{ is relative prime.}

**Proof:** Each $q \in Q$ is prime and therefore not divisible by the first $n$ primes $p_1..p_n$. 

\[
f(q) = \left(\begin{array}{c} q \mod 2 \\ q \mod 3 \\ q \mod 5 \\ \vdots \\ q \mod p_n \end{array}\right)
\]
has no zero value in its tuple and therefore is relative prime. 

**Remark:** $f(1) = \left(\begin{array}{c} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{array}\right)$ is never prime in $PM(n)$.

In PM(2) and PM(3) all relative prime elements (except 1) are prime. 
For $n \geq 4$ there are many other relative prime elements in PM(n), that are not prime. 
In PM(4) (range 11..210) all examples for this are 

\[
11^2 = 121 = \left(\begin{array}{c} 1 \\ 1 \\ 2 \end{array}\right), 11 \ast 13 = 143 = \left(\begin{array}{c} 1 \\ 2 \\ 3 \end{array}\right), \\
11 \ast 17 = 187 = \left(\begin{array}{c} 1 \\ 1 \\ 6 \end{array}\right), 13^2 = 169 = \left(\begin{array}{c} 1 \\ 4 \\ 1 \end{array}\right), 11 \ast 19 = 209 = \left(\begin{array}{c} 1 \\ 4 \\ 6 \end{array}\right).
\]

**Lemma 3.3** Let $p_{n+1}$ be the $(n+1)$-th prime number in $N$. Each relative prime number $t \in PM(n)$ with $f^{-1}(t) = k$ and $p_{n+1} \leq k < p_{n+1}^2$ is prime.

**Proof:** Each relative prime number in PM(n) is not divisible by the first $n$ primes. Therefore the minimal relative prime number $q$, that is not prime must have $f^{-1}(q) = p_{n+1}^2$. 

6
Lemma 3.4 Given the set $PM(n)$. We define the subset

$PM'(n) := \{ t \in PM(n) \mid t \text{ is not prime} \land \text{minimal prime factor } (f^{-1}(t)) > p_n \}$

$PM'(n)$ contains all relative prime elements that are not prime.

Proof: With minimal prime factor $(f^{-1}(t)) > p_n =>$

all tuple values are $>0 =>$

t is relative prime per definitionem. $lacksquare$

Proposition 1 Let $p_{n+1}$ be the $(n+1)$-th prime number in $N$. The number of all primes $q$ with $p_{n+1} \leq q < \prod_{i=1}^{n} p_i$ is

$$\prod_{i=1..n} (p_i - 1) - 1 - \text{size of } PM'(n)$$

Proof: The number of relative primes in $PM(n)$ is $\prod_{i=1..n} (p_i - 1)$.

From this we subtract one for the relative prime $1 = \begin{pmatrix} 1 \\ 1 \\ \ldots \\ 1 \end{pmatrix}$. The remaining relative primes, that are not prime are defined in the set $PM'(n)$. $lacksquare$

Example: The number of primes between 6 and 30: $(1*2*4) - 1 - 0 = 7$
The number of primes between 10 and 210: $(1*2*4*6) - 1 - 5 = 42$.

Corollary 1 Let $p_{n+1}$ be the $(n+1)$-th prime number in $N$. The number of all primes $q$ with $q < \prod_{i=1}^{n} p_i$ is

$$n + \prod_{i=1..n} (p_i - 1) - 1 - \text{size of } PM'(n)$$

4 the inverse function $f^{-1}$

Definition: Let the set $PM(n)$ be given. We define the unary elements in $PM(n)$ as all elements with (n-1) zeros and one 1 in the tuple.

Example: There are $n$ unary tuples in $PM(n)$. In $PM(4)$ there are 4 unary elements

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$
Lemma 4.1 Each unary element in PM(n) generates a subset of PM(n) that is a finite field. Therefore each element t in this subset has an inverse element.

Proof: Let

\[ PM(n)_{ui} := \{ \begin{pmatrix} 0 \\ \vdots \\ k \\ \vdots \\ 0 \end{pmatrix} | k \in \{0, \ldots, p_i - 1\} \} \]

be the subset of all tuples, where all tuple values are zero, but on the i-th position. This subset forms a field with addition and multiplication and is isomorphic to the finite field Z/Z_{p_i}.

Lemma 4.2 Each element in PM(n) can be constructed by the unary elements.

Proof:

\[
\begin{pmatrix} k_1 \mod 2 \\ k_2 \mod 3 \\ k_3 \mod 5 \\ \vdots \\ k_n \mod p_n \end{pmatrix} = \sum_{i=1}^{k_1} \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \end{pmatrix} + \sum_{i=1}^{k_2} \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix} + \cdots + \sum_{i=1}^{k_n} \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}
\]

Definition: Let the finite field Z/Z_{p_i} with p_i prime be given. For each element \( t \in Z/Z_{p_i} \) there exists an inverse element \( t^{-1} \) with \( t \cdot t^{-1} = 1 \).

We define \( t \modInverse(p_i) := t^{-1} \)

Proposition 1 For an unary element \( u_i \in PM(n) : v_i := f^{-1}(u_i) \) can be calculated by:

\[
v_i = \left( \prod_{j=1}^{n} p_j \right) / p_i \cdot \left[ \left( \prod_{j=1}^{n} p_j \right) / p_i \modInverse(p_i) \right]
\]

Proof: The value \( v_i = f^{-1}(u_i) \) must be

[condition a]: divisible by all primes \( p_j, j \in \{1..n\}, j \neq i \) except \( p_i \)

and [condition b]: \( v_i \mod (p_i) = 1 \).

\( v_i := (\prod_{j=1}^{n} p_j / p_i) \) resolves condition a, but not in all cases condition b.

\( v_i := (\prod_{j=1}^{n} p_j / p_i) \) mod \( p_i = 1 \) resolves both conditions.
\(v_i\) is an element in the field \(PM(n)\). Therefore there exists an inverse element.

Due to the isomorphism in chapter 2 there can only be one \(v_i^*\) with \(f(v_i) = u_i\).

Theorem 1 (inverse function) Let \(PM(n)\) be given.
Let \(g: PM(n) \to F \prod_p\) :

Let the map be defined by

\[
g(\begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ \vdots \\ t_n \end{pmatrix}) = (\sum_{i=1..n} t_i \cdot v_i) \mod (\prod_{i=1}^n p_i)
\]

Then \(g\) is the inverse function to \(f\).

Proof: Each \(k \in PM(n)\) can be calculated by its unary elements. For each unary element the value \(v_i\) is known.

Remark: For all \(t_i = 0 \to g(t) = 0\). In \(F \prod p_i\) this is equivalent to \(\prod p_i\).

Example:

| n | range | rel. primes | coeffs |
|---|-------|-------------|--------|
| 1 | 1 - 2 | 1           | \(f^{-1}(t) = (1t_1) \mod 2\) |
| 2 | 1 - 6 | 2           | \(f^{-1}(t) = (3t_1 + 4t_2) \mod 6\) |
| 3 | 1 - 30| 8           | \(f^{-1}(t) = (15t_1 + 10t_2 + 6t_3) \mod 30\) |
| 4 | 1 - 210| 48          | \(f^{-1}(t) = (105t_1 + 70t_2 + 126t_3 + 120t_4) \mod 210\) |
| 5 | 1 - 2310| 480        | \(f^{-1}(t) = (1155t_1 + 1540t_2 + 1386t_3 + 330t_4 + 210t_5) \mod 2310\) |

with \(t_1 \in \{0,1\}\), \(t_2 \in \{0,1,2\}\), \(t_3 \in \{0,1,2,3,4\}\), \(t_4 \in \{0,1,2,3,4,5,6\}\), \(t_5 \in \{0,1,2,3,4,5,6,7,8,9,10\}\)

5 conclusions

The inverse function provides an algorithm to test for higher primes:

We can iterate all relative prime elements in \(PM(n)\) to calculate all relative prime values up to \(\prod_{i=1}^n p_i\).

Start for example with \(\begin{pmatrix} 1 \\ 2 \\ 4 \\ 6 \end{pmatrix}\) and subtract one from the last value \(\begin{pmatrix} 1 \\ 2 \\ 4 \\ 5 \end{pmatrix}\), \(\begin{pmatrix} 1 \\ 4 \end{pmatrix}\), ...

until \(\begin{pmatrix} 1 \\ 2 \\ 4 \\ 1 \end{pmatrix}\) and then switch to \(\begin{pmatrix} 1 \\ 2 \\ 3 \\ 6 \end{pmatrix}\) and then repeat until we reach \(\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}\).
For each element we can calculate \( f^{-1}(t) \) as a prime candidate. This is really similar to the wheel factorization of primes, but not in sequential order. Instead of iterating the wheel multiple times we just go up to \( \prod_{i=1}^{n} p_i \).

There are some questions open to make this algorithm effective. We still have to check each relative prime element for its primeness. As part of a solution, it is possible to extend each element

\[
t = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix} \in PM(n)
\]

for tuple positions \( t_i > n \). Together with \( f^{-1}(t) \leq \prod_{i=1}^{n} p_i \) these extensions are unique.

The extended element \( t' = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \\ t_{n+1} \\ \vdots \\ t_{n+m} \end{pmatrix} \) can be easily checked for primeness.

### 6 remarks

Thanks to all the reviewers for their valuable feedback. A special thanks to Ralf Schiffler (University of Connecticut) for his help with the calculation of the inverse function.

After publication of this article Ramin Zahedi contacted me with his own article, which provides similar results from a different perspective.[1]

### References

[1] R. Zahedi, On algebraic structure of the set of prime numbers, 2012; [arXiv:1209.3165v5](arXiv:1209.3165v5)