1 Product and Sum of Two Primes

We noticed in [**?**], that $2, 3 \mid n+1$ if and only if $2, 3 \mid r$ for any prime greater than 3, this is not true. Let h be an odd prime greater than 3, *if* $h \mid n+1$ *, then it is not necessary that* h $\mid r$

Proof.
Let h be prime greater than 3, then $h - 1 = 2\frac{h-1}{2}$ where $\frac{h-1}{2} \geq 2$. Let $n = pq$, where p and q are odd primes such that:
$p = 2h$ and $q = \frac{h-1}{2}h$, then $n = pq = 2\frac{h-1}{2} = -1h$, so $n+1 = 0h$, then $h \mid n+1$ but $rh = p + qh = 2 - 2^{-1} = 2^{-1}(4 - 1) = 2^{-1}3 \neq 0h$, so $h \nmid r$. □

Let $h = 7$, $n = 3639$, then $7 \mid n+1$ and $r7 = (p+q)7 = 5$, so $7 \nmid r$. in fact, if $n + 1 = 07$, then $r7$ could have one of the values: $0, 2$ or 5. In general, there is a relation between nh and rh. for example: let $h = 7$, then the following table contains the possible values of $r7$, for each $n7 \neq 1$.

Table 1: $n7$

$n7$	$r7$
1	1, 2, 5, 6
2	1, 3, 4, 6
3	0, 3, 4
4	2, 3, 4, 5
5	0, 1, 6
6	0, 2, 5

As shown in table **??** if $n7 \neq 0$, then $r7$ has either 3 or 4 values. In general, for any odd prime h, if $nh \neq 0$, then rh has $\frac{h-1}{2}$ or $\frac{h+1}{2}$ different values.
Let h be prime and a,b,c,$d \in \mathbb{Z}_h^*$ be distinct mod h If ab = cd h, then a+b $\neq c + dh$

Proof.
Let a,b,c,$d \in \mathbb{Z}_h^*$ and distinct with $ab = cdh$.
Suppose $a + b = c + dh$ then $a = c + d - bh$

$$(c + d - b)b = cdh$$

$$cb + db - b^2 = cdh$$

$$db - b^2 = cd - cbh$$

$$(d - b)b = c(d - b)h$$

$$(d - b)b = (d - b)ch$$

Since $d - b \neq 0h$ which means $b = ch$. However, this contradicts the assumption, So $a + b \neq c + dh$ □

Let $n = pq$ and $r = p + q$ where p, q, h are distinct odd primes With $n \neq 0 \bmod h$ then: r $\bmod h has \frac{h-1}{2} or \frac{h+1}{2} different possible values.$

Proof.
Let $a \in \mathbb{Z}_h$. a is a quadratic residue modulo h if $\exists x \in \mathbb{Z}_h^*$ such that $a = x^2 h$. If a isn't a quadratic residue then for any $b \in \mathbb{Z}_h^*$, $\exists c \neq b \in \mathbb{Z}_h^*$ such that $bc = ah$.

$$b_1 c_1 = b_2 c_2 = ... = b_{h-1} c_{h-1} = ah$$

Since the multiplication and addition is commutative, the above becomes:

$$b_1 c_1 = b_2 c_2 = ... = b_{\frac{h-1}{2}} c_{\frac{h-1}{2}} = ah$$

So by lemma **??**: $b_i + c_i \neq b_j + c_j$ if $i \neq j$ then we have $\frac{h-1}{2}$ different rh.

Now, suppose a is a quadratic residue then $\exists x \in \mathbb{Z}_h^*$, such that $a = x^2 h$, and $a = (h - x)^2 h$ so we have

$$b_1 c_1 = b_2 c_2 = ... = b_{\frac{h-3}{2}} c_{\frac{h-3}{2}} = b^2_{\frac{h-1}{2}} = b^2_{\frac{h+1}{2}} = ah$$

So we have $\frac{h+1}{2}$ different rh □

The ideas described above hint on the algorithm's dependence on pre-computation, and there are several aspects to consider. How far can we pre-process? and whether it is useful to go to such lengths. To calculate $r \bmod h$ for all $n \bmod h$, one can find the Cayley tables for multiplication and addition then save the unique values in a manner similar to that of table **??**.

1.0.1 Exhaustive Listing

It is also possible to use a more efficient listing algorithm. We search all useful combinations with second terms greater than or equal to the first term then store the possible values as lists with their corresponding $n \bmod p$ as keys to those lists as in **??**

Algorithm 1 Listing

Require: $h \leftarrow prime \geq 7$
for i in $[1, p-1]$ **do**
  for j in $[i, p-1]$ **do**
    $permval[ij + 1] \leftarrow (i + j)p$
  end for
end for

1.0.2 'r' for a Specific '$n \bmod h$'

Let $x = n \bmod h$ and $r = i + i^{-1}x$ where $i \in \mathbb{Z}_h^*$

Proof.

$$ij = x \bmod h$$

$$j = xi^{-1} \bmod h$$

$$r = i + j = xi^{-1} \bmod h$$

Notice if $r \bmod h$ is a possible value, then $(-r) \bmod h$ is also a possible value. Since $-r = -(xi^{-1} + i) = -xi^{-1} - i = x(-i)^{-1} - i$ ☐

1.0.3 Using Inverse

Algorithm 2 Using $n \bmod h$ multiplied by i^{-1}

Require: h, n
Ensure: $h \geq 7$

for i in $[1, h-1]$ **do**
  if $iinni\_list$ **then**
    continue
  end if
  $ni \leftarrow n * i^{-1} \bmod h$
  append ni to ni_list
  $r \leftarrow (i + ni) \bmod h$
  if $rinr\_list$ **then**
    continue
  end if
  append r to r_list
  if $r \neq 0$ **then**
    append $(h - r)$ to r_list
  end if
end for

2 Divisibility by 8

Let p and q be distinct odd primes, $n = pq$, and $r = p + q$ then: $8 \mid n + 1 ifandonlyif 8 \mid r$

Proof. Let p and q be two distinct odd primes, then they have one of the forms:

1. $8k + 1$
2. $8k + 3$
3. $8k + 5$
4. $8k + 7$

then the possible forms of n:

1. $[t](8k+1)(8m+1) = 64km + 8(k+m) + 1$
   $= 8k' + 1$

2. $[t](8k+1)(8m+3) = 64km + 8(3k+m) + 3$
   $= 8k' + 3$

3. $[t](8k+1)(8m+5) = 64km + 8(5k+m) + 5$
   $= 8k' + 5$

4. $[t](8k+1)(8m+7) = 64km + 8(7k+m) + 7$
   $= 8k' + 7$

5. $[t](8k+3)(8m+3) = 64km + 24(k+m) + 9$
   $= 8k' + 1$

6. $[t](8k+3)(8m+5) = 64km + 8(5k+3m) + 15$
   $= 8k' + 7$

7. $[t](8k+3)(8m+7) = 64km + 8(7k+5m) + 21$
   $= 8k' + 5$

8. $[t](8k+5)(8m+5) = 64km + 40(k+m) + 25$
   $= 8k' + 1$

9. $[t](8k+5)(8m+7) = 64km + 8(7k+5m) + 35$
   $= 8k' + 3$

10. $[t](8k+7)(8m+7) = 64km + 56(k+m) + 49$
    $= 8k' + 1$

and the possible forms of r will respectively be:

a) $[t](8k+1) + (8m+1) = 8(k+m) + 2$
   $= 8k' + 2$

b) $[t](8k+1) + (8m+3) = 8(k+m) + 4$
   $= 8k' + 4$

c) $[t](8k+1) + (8m+5) = 8(k+m) + 6$
   $= 8k' + 6$

d) $[t](8k+1) + (8m+7) = 8(k+m+1)$
   $= 8k'$

e) $[t](8k+3) + (8m+3) = 8(k+m) + 6$
   $= 8k' + 6$

f) $[t](8k+3) + (8m+5) = 8(k+m+1)$
   $= 8k'$

g) $[t](8k+3) + (8m+7) = 8(k+m) + 10$
   $= 8k' + 2$

h) $[t](8k+5)+(8m+5) = 8(k+m)+10$
$= 8k'+2$

i) $[t](8k+5)+(8m+7) = 8(k+m)+12$
$= 8k'+4$

j) $[t](8k+7)+(8m+7) = 8(k+m)+14$
$= 8k'+6$

Here $n+1$ is divisible by 8 for the fourth and sixth forms, and similarly the corresponding forms of r are also divisible by 8. The other forms for $n+1$ and their corresponding forms for r are not divisible by 8. Therefore, we conclude that $8 \mid n+1$ *if and only if* $8 \mid r$ $\square$

We also extend previous results in a similar fashion applicable on semi-primes equal to 3 or 710 as shown in the following tables.

Table 2: $n = 310$

Tens odd	
$3 \mid n+1$	$3 \nmid n+1$
$r = 60k+54$	$r = 60k+14$
$r = 60k+6$	$r = 60k+34$
	$r = 60k+26$
	$r = 60k+46$

Tens even			
$8 \mid n+1$		$8 \nmid n+1$	
$3 \mid n+1$	$3 \nmid n+1$	$3 \mid n+1$	$3 \nmid n+1$
$r = 120k+24$	$r = 120k+64$	$r = 120k+84$	$r = 120k+4$
$r = 120k+96$	$r = 120k+104$	$r = 120k+36$	$r = 120k+44$
	$r = 120k+16$		$r = 120k+76$
	$r = 120k+56$		$r = 120k+116$

Table 3: $n = 710$

Tens odd	
$3 \mid n+1$	$3 \nmid n+1$
$r = 60k + 18$	$r = 60k + 38$
$r = 60k + 42$	$r = 60k + 58$
	$r = 60k + 2$
	$r = 60k + 22$

Tens even			
$8 \mid n+1$		$8 \nmid n+1$	
$3 \mid n+1$	$3 \nmid n+1$	$3 \mid n+1$	$3 \nmid n+1$
$r = 120k + 48$	$r = 120k + 8$	$r = 120k + 108$	$r = 120k + 68$
$r = 120k + 72$	$r = 120k + 88$	$r = 120k + 12$	$r = 120k + 28$
	$r = 120k + 32$		$r = 120k + 92$
	$r = 120k + 112$		$r = 120k + 52$

3 Formulas and Prime Fields

For any formula $r(k) = ak + b$ in [?], and a prime $h \geq 7$. r(k) = r(m) $\mod hifandonlyifk = m \mod h$

Proof.
Let $r(k) = ak + bh$, with h a prime, and $a = 2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}$, then:

$$r(k) = r(m)h$$
$$\iff ak + b = am + bh$$
$$\iff ak = amh$$
$$\iff k = mh$$

□

From proposition **??** we have:

1. $r(k) \mod h$, $r(k+1) \mod h$, ..., $r(k+h-1) \mod h$ are distinct, so $\mathrm{Z}_h = \{r(k) \mod h, ..., r(k+h-1)\}$ then $\frac{h-1}{2}$ or $\frac{h+1}{2}$ of $r(k)$, $r(k+1)$, ..., $r(k+h-1)$ cannot be equal to $p+q$. In the previous example $n = 3639$ and $n \mod 7 = 6$, the possible values of $r \mod 7$ are 0,2, and 5 as shown in table **??**. So, if $r(k) \mod 7 = 3$, then $r(k) \neq p + q$

2. If $r(k) \mod h \neq$ one of the possible values of $r \mod h$, then $r(k+\gamma h) \neq$ one of the possible values of $r \mod h$. If $r(k) \mod 7 = 3$, then by proposition **??**, $r(k+7\gamma) \mod 7 = 3$. So, $r(k+7\gamma) \neq p+q$.

The method suggested in [?] is to compute the starting points for a number of predefined formulas $r_i(k)$ using $\lceil 2\sqrt{n} \rceil$, the formulas are chosen depending on certain characteristics of 'n'. After which, the condition

$$r_i(k) = p + q \iff \sqrt{r^2 - 4n isapositiveinteger} \tag{1}$$

, is checked while iteratively incrementing k.

For example, given $n = 234948664218045611$ (computed from $p = 925106617$ and $q = 253969283$) we choose the table 6 from [?]. Compute the starting points for each of the three formulas $r_1(k_{1,0})$, $r_2(k_{1,0})$, $r_3(k_{3,0})$ using $2\sqrt{n} \approx 969430068$. Check the condition $r_i(k) = p+q \iff \sqrt{r^2 - 4n}$ is a positive integer iteratively while incrementing k.
The value for k that satisfy the condition is $k_{3,1747048} = 9825632$
$r_3(9825632) = 1179075900$.
Number of tries $= 3 \times 1747048 = 5241144$

Using the results from proposition **??**, one can approximately halve the number of expensive condition checks in the previous method. Computing modulo h operations h times then only checking the condition for the values in a permissible congruence class modulo h. The decrease in the number of condition checks depend on whether 'n' is a quadratic residue modulo h which is discussed in depth later in **??**.

3.1 Example (with $h = 7$)

Given $n = 234948664218045611$
Rather than evaluating $r_1(k), r_2(k), r_3(k)$ starting with the above values for $k_{1,0}, k_{2,0}, k_{3,0}$ respectively then continuing to increment the k's until $\sqrt{r^2 - 4n}$ is equal to an integer, we use proposition **??** with $h = 7$, then compute $nh = 1$ and evaluate the first h values of $(k_{1,i}, k_{2,i}, k_{3,i})$. After which, we check if they map to the possible values modulo h as shown in table **??**, if not we discard the value.

Table 4: First 7 iterations of the example

i	$r_1(k)$	$r_2(k)$	$r_3(k)$
0	969430212 mod $h = 2$	969430188 mod $h = 6$	~~969430140 mod $h = 0$~~
1	~~969430812 mod $h = 0$~~	~~969430788 mod $h = 4$~~	969430260 mod $h = 1$
2	969431412 mod $h = 5$	969431388 mod $h = 2$	969430380 mod $h = 2$
3	~~969432012 mod $h = 3$~~	~~969431988 mod $h = 0$~~	~~969430500 mod $h = 3$~~
4	969432612 mod $h = 1$	969432588 mod $h = 5$	~~969430620 mod $h = 4$~~
5	969433212 mod $h = 6$	~~969433188 mod $h = 3$~~	969430740 mod $h = 5$
6	~~969433812 mod $h = 4$~~	969433788 mod $h = 1$	969430860 mod $h = 6$

Discard all values $r(k + \gamma h)$ corresponding to the first h values crossed as shown in the above table. Traverse the remaining space until a value of r(k) that satisfies the condition is reached. The value for k where a solution exists is $k_{3,1747048} = 9825632$.

- Number of tries = $\lceil \frac{4}{7} 5241144 \rceil$

3.2 Choosing a prime h

Given two primes h_1 and h_2, where $h_1 \nmid n$ and $h_2 \nmid n$. Choosing the prime that has rh with $\frac{h-1}{2}$ values is generally better than choosing a prime with $\frac{h+1}{2}$ values. For any two primes such that $h_2 > h_1$ and both have $\frac{h-1}{2}$ congruence classes, it is better to use h_1. However, if both primes h_1 and h_2 had $\frac{h+1}{2}$ values for rh we choose h_2.

4 Multiple Prime Fields

Let h_1, h_2 be odd distinct primes, $\mathbb{Z}_{h_2} = \{0, ..., h_2 - 1\}$ and $K = \{r(k + \gamma h_1) \bmod h_2 \mid \gamma \in \mathbb{Z}_{h_2}\}$ then $K = \mathbb{Z}_{h_2}$

Proof.
Suppose $r(k + \gamma_1 h_1) \bmod h_2 = r(k + \gamma_2 h_1) \bmod h_2$

$$(a(k + \gamma_1 h_1) + b) \bmod h_2 = (a(k + \gamma_2 h_1) + b) \bmod h_2$$

$$a(k + \gamma_1 h_1) \bmod h_2 = a(k + \gamma_2 h_1) \bmod h_2$$

$$k + \gamma_1 h_1 \bmod h_2 = k + \gamma_2 h_1 \bmod h_2$$

$$\gamma_1 h_1 \bmod h_2 = \gamma_2 h_1 \bmod h_2$$

$$\gamma_1 \bmod h_2 = \gamma_2 \bmod h_2 contradiction.$$

□

By proposition **??**:

$$r(k) \bmod h_1 = r(k + \gamma h_1) \bmod h_1$$

So, if $r(k) \bmod h_1$ is one of the possible values, then $r(k + \gamma h_1)$ is also one of the possible values, but $\frac{h_2-1}{2}$ or $\frac{h_2+1}{2}$ of $r(k), r(k + h_1), ..., r(k + (h_2 - 1)h_1)$ are not of the possible values modulo h_2 then the number of tries decreases by $\frac{h_2-1}{2h_2}$ or $\frac{h_2+1}{2h_2}$ of the number of tries.

Table 5: $n13$

$n13$	$r13$
1	0, 1, 2, 4, 9, 11, 12
2	2, 3, 5, 8, 10, 11
3	0, 3, 4, 5, 8, 9, 10
4	0, 2, 4, 5, 8, 9, 11
5	2, 4, 6, 7, 9, 11
6	1, 5, 6, 7, 8, 12
7	1, 4, 5, 8, 9, 12
8	3, 4, 6, 7, 9, 10
9	0, 1, 3, 6, 7, 10, 12
10	0, 1, 2, 6, 7, 11, 12
11	1, 2, 3, 10, 11, 12
12	0, 3, 5, 6, 7, 8, 10

4.1 Example (with $h_1 = 7$, $h_2 = 13$)

$n = 234948664218045611$
$nh_1 = 1$
$nh_2 = 2$

Table 6: First 13 iterations of the example

	$r_1(k) = 600k_1 + 12$			$r_2(k) = 600k_2 + 588$			$r_3(k) = 120k_3 + 60$		
i	$r_1(k)$	modh_1	modh_2	$r_2(k)$	modh_1	modh_2	$r_2(k)$	modh_1	modh_2
0	969430212	2	10	~~969430212~~	6	~~12~~	~~969430212~~	~~0~~	3
1	~~969430812~~	~~0~~	~~12~~	~~969430788~~	~~4~~	~~1~~	~~969430260~~	1	~~6~~
2	~~969431412~~	5	~~1~~	969431388	2	3	969430380	2	~~9~~
3	~~969432012~~	~~3~~	3	~~969431988~~	~~0~~	5	~~969430500~~	~~3~~	~~12~~
4	969432612	1	5	~~969432588~~	5	~~7~~	~~969430620~~	~~4~~	2
5	~~969433212~~	~~6~~	~~7~~	~~969433188~~	~~3~~	~~9~~	969430740	5	5
6	~~969433812~~	~~4~~	~~9~~	969433788	1	11	969430860	6	8
7	969434412	2	11	~~969434388~~	6	~~0~~	~~969430980~~	~~0~~	11
8	~~969435012~~	~~0~~	~~0~~	~~969434988~~	~~4~~	2	~~969431100~~	1	~~1~~
9	969435612	5	2	~~969435588~~	2	~~4~~	~~969431220~~	2	~~4~~
10	~~969436212~~	~~3~~	~~4~~	~~969436188~~	~~0~~	~~6~~	~~969431340~~	~~3~~	~~7~~
11	~~969436812~~	1	~~6~~	969436788	5	8	~~969431340~~	~~4~~	10
12	969437412	6	8	~~969437388~~	~~3~~	10	~~969431340~~	5	~~0~~

Number of tries $= \lceil \frac{4\times 6}{7\times 13} 5241144 \rceil$

Let $h_1, h_2, ...h_d$ be distinct odd primes, and $x = \prod_{i=1}^{d-1} h_i$ then $\mathbb{Z}_{h_d} = \{0, ..., h_d - 1\}$ and let $K = \{r(k + \gamma x) \bmod h_d \mid \gamma \in \mathbb{Z}_{h_d}\}$ then $K = \mathbb{Z}_{h_d}$

Proof.

$$r(k+\gamma_1 x) = r(k+\gamma_2 x) \bmod h$$

$$a(k+\gamma_1 x) + b = a(k+\gamma_2 x) + b \pmod h$$

$$a(k+\gamma_1 x) = a(k+\gamma_2 x) \bmod h$$

$$k+\gamma_1 x = k+\gamma_2 x \pmod h$$

$$\gamma_1 x = \gamma_2 x h$$

$$\gamma_1 = \gamma_2 h$$

□

4.2 Complexity Analysis

For $b = \log_2(p-q)$
in the worst case $b \approx \log_2(n) - 1$
The factoring algorithm is split into two main parts a setup and search.

4.2.1 Complexity of The Setup Part

Given $h_1, ..., h_i$ primes ≥ 7 and their corrosponding possible $r \bmod h_i$ values. There are on average $\approx \frac{h_i}{2}\ r_{j,i}$ values for any $x_i = n \bmod h_i$. The complexity of a single 'mod' operation is roughly of the form $O(b\log_2(h_i))$. For each h_i the mod operation is computed h_i times. In total there are $\sum_i h_i$ mod operations in the setup phase. So, the complexity of the setup part is:

$$O(\sum_i h_i b \log_2 h_i)$$

Assumming $i = b$

$$O(\sum_{i=1}^{b} h_i b \log_2 h_b)$$

4.2.2 Complexity of The Search Part

Initially the search part without the setup part made a condition check for each iteration and asumming each condition check necessitates a square root computation. $O[(2b)^2]$ condtion checks in the search part are made $c(p-q)$ times.

$$O[2^b(2b)^2]$$

After adding the setup phase the nubmer of square root computations becomes $\approx \frac{c(p-q)}{2}$

$$O(\frac{2^b}{2^i}(2b)^2)$$

assuming $i = b$ is used $O((2b)^2)$ The total expression:

$$O(\sum_i h_i b \log_2 h_i) + O(\frac{2^b}{2^i}(2b)^2))$$

for $i = b$

$$O(\sum_{i=0}^{b} blog_2 h_b + ((2b)^2))$$

$$O((b \log_2(h_b)^2 + 4b^2))$$

$$O(b^2(4 + \log_2(h_b)^2))$$

5 Hello this is section

testj jthe rest of the document l testj jthe rest of the document l