Construction of Composite Numbers by Recursively Exponential Numbers

SZE, Tsz Wo

November 23, 2005

1 Introduction

In this paper, we give some constructions of composite numbers N, such that every number less than or equal to M divides N. Therefore,

$$\mathrm{lcm}(1, 2, 3, \cdots, M) \mid N.$$

We call such numbers *divisible up to M*.

Definition 1.1. *An integer N is divisible up to M if $n \mid N$ for all $0 < n \leq M$.*

A trivial construction is $N = M!$. However, it requires an enumeration of all prime numbers less than or equal to M. The constructions given in this paper do not require such enumeration.

In section 2, we present a family of constructions of the composite number $D_{r,k}$, where $D_{r,k}$ is divisible up to $2^{k-1} - 1$ for any positive integer r. The factoring problem is discussed in section 3. The problem of computing $D_{r,k}$ mod n is closely related to the factoring problem. They are probably equivalent.

2 Numbers of the form $r^E - E$, where $E = r^{r^{\cdot^{\cdot^{\cdot^{r}}}}}$

Let $r \in \mathbb{N} = \{1, 2, \cdots\}$. Define *recursively exponential numbers*, $E_{r,k}$, to be

$$E_{r,-1} = 0, \tag{2.1}$$
$$E_{r,k} = r^{E_{r,k-1}} \quad \text{for } k \geq 0. \tag{2.2}$$

Let $D_{r,k}$ be the difference between $E_{r,k}$ and $E_{r,k-1}$, i.e.

$$D_{r,k} = E_{r,k} - E_{r,k-1} \quad \text{for } k \geq 0. \tag{2.3}$$

$D_{r,k}$ can be evaluated by the recursive equation below.

$$D_{r,k} = E_{r,k-1}(r^{D_{r,k-1}} - 1) \quad \text{for } k \geq 0. \tag{2.4}$$

Table 2.1 shows some values of $E_{r,k}$ and $D_{r,k}$. $E_{r,k}$ and $D_{r,k}$ grow repidly. Obviously, $E_{r,k}$ divides $E_{r,k+1}$ for $k \geq 1$. The divisibe relationship also holds for $D_{r,k}$. We have the following proposition.

k	$E_{2,k}$	$D_{2,k}$	$E_{3,k}$	$D_{3,k}$	$\cdots$	$E_{r,k}$	$D_{r,k}$
0	1	1	1	1	$\cdots$	1	1
1	2	1	3	2	$\cdots$	r	$r-1$
2	4	2	27	24	$\cdots$	r^r	$r^r - r$
3	16	12	7625597484987	7625597484960	$\cdots$	r^{r^r}	$r^{r^r} - r^r$

Table 2.1: Examples of $E_{r,k}$ and $D_{r,k}$

Proposition 2.1. *For $r > 1$ and $0 \leq a < b$,*

$$D_{r,a} \mid D_{r,b}. \tag{2.5}$$

Proof. It is enough to show $D_{r,k} \mid D_{r,k+1}$ for $k \geq 0$. Then, the theorem follows.

We show it by induction. $D_{r,0} = 1$ divides $D_{r,1} = r-1$. Assume $D_{r,k-1} \mid D_{r,k}$. For $k > 0$, let $D_{r,k} = nD_{r,k-1}$ for some integer n. By equation 2.4,

$$\begin{aligned} D_{r,k+1} &= E_{r,k}(r^{D_{r,k}} - 1) \\ &= E_{r,k}(r^{nD_{r,k-1}} - 1) \\ &= E_{r,k}(r^{D_{r,k-1}} - 1)(r^{(n-1)D_{r,k-1}} + r^{(n-2)D_{r,k-1}} + \cdots + 1). \end{aligned}$$

Obviously, $E_{r,k-1} \mid E_{r,k}$. Therefore, $D_{r,k} = E_{r,k-1}(r^{D_{r,k-1}} - 1)$ divides $D_{r,k+1}$. □

The next proposition helps to show $D_{r,k}$ is divisible up to $2^m - 1$ for some m in later sections. The Euler's totient function is denoted by $\phi(n)$, which is the number of positive numbers less than or equal to n and prime to n. $\mathrm{ord}_n(r)$ denotes the order of r in the ring $\mathbb{Z}_n$.

Proposition 2.2. *Let $r > 1$ be an integer. Suppose the following hypotheses.*

(i) 6 divides $D_{r,b}$ for some $b \geq 2$.

(ii) If, for some $k \geq 2$, every k-bit integer divides $D_{r,b+k-2}$, then $\phi(a)$ divides $D_{r,b+k-2}$ for $2^k \leq a < 2^{k+1}$ with $\gcd(r, a) = 1$,

Then, for any $n \in \mathbb{N}$, if $n < 2^m$, then $n \mid D_{r,b+m-2}$.

Proof. Let $n = \prod_{i=0}^{l} p_i^{e_i}$ be a factorization of n, where p_i are distinct primes. Consider the case that all p_i divides r. $\sum_{i=0}^{l} e_i < m$ since $n < 2^m$. Then, $n \mid r^{m-1}$. It is clear that $r^{m-1} \mid E_{r,m-1}$. With equation (2.4), $n \mid D_{r,m}$. By proposition 2.1, $n \mid D_{r,b+m-2}$.

The other case is proven by induction. For $m = 2$, 6 divides $D_{r,b}$ by hypothesis (i). The theorem is true for $m = 2$. Assume all k-bit numbers divide $D_{r,b+k-2}$ for some $k \geq 2$. Since $D_{r,b+k-2} \mid D_{r,b+k-1}$ by proposition 2.1, it is enough to show $n \mid D_{r,b+k-1}$ for $2^k \leq n < 2^{k+1}$.

If $\gcd(r, n) > 1$, write $n = st$, such that $\gcd(r, t) = 1$, $t > 1$ and each prime factor of s divides r. $s > 1$ implies $t < 2^k$. Similarly, $t > 1$ implies $s < 2^k$. Then, $s \mid D_{r,b+k-2}$ and $t \mid D_{r,b+k-2}$ by induction assumption. $\gcd(s, t) = 1$ implies $st \mid D_{r,b+k-2}$. Therefore, $n \mid D_{r,b+k-1}$ by proposition 2.1.

For the case that $\gcd(r, n) = 1$, $\phi(n) \mid D_{r,b+k-2}$ by hypothesis (ii). We have $\mathrm{ord}_n(r) \mid \phi(n)$ as a consequence of Lagrange's theorem. Together with the fact $n \mid (r^{\mathrm{ord}_n(r)})^c - 1$ for any positive integer c, we have n divides $E_{r,b+k-2}(r^{D_{r,b+k-2}} - 1) = D_{r,b+k-1}$. □

2.1 The case $r = 2$

In this section, $E_{2,k} = \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{k}$ is denoted by E_k and $D_{2,k} = E_k - E_{k-1}$ is denoted by D_k. The sequences $\{E_k\}_k$ and $\{D_k\}_k$ are known as Sloane's A14221 and A038081 [4]. D_k also is the number of rooted identity trees of height k and the number of sets of rank k.

2.1.1 Ackermann function

E_k and D_k can be evaluated by *Ackermann function*. Ackermann function $A(m, n)$ is defined by

$$A(m,n) = \begin{cases} n+1 & \text{if } m = 0, \\ A(m-1, 1) & \text{if } m > 0 \text{ and } n = 0 \\ A(m-1, A(m, n-1)) & \text{if } m > 0 \text{ and } n > 0. \end{cases}$$

It can be shown that $A(4, n) = \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n+3} - 3$. Therefore, for $k \geq 4$,

$$E_k = A(4, k-3) + 3 \quad (2.6)$$
$$D_k = A(4, k-3) - A(4, k-4). \quad (2.7)$$

2.1.2 Divisibility of D_m

D_{m+1} is divisible up to $2^m - 1$, which is a special case of theorem 2.8. In other words, all m-bit positive integers divide D_{m+1}. The table below shows the factorization of D_m for the first few cases. It is clear that the factorization of D_m contains all primes up to $2^{m-1} - 1$.

m	E_m	D_m	Factorization of D_m
0	1	1	1
1	2	1	1
2	4	2	2
3	16	12	$2^2 \cdot 3$
4	65536	65520	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$
5	2^{65536}	$2^{65536} - 65536$	$2^{16} \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13^2 \cdot 17 \cdot 19 \cdot 29 \cdot 31$ $\cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 61 \cdot 71 \cdot 73 \cdot 79 \cdot 97 \cdots$

Table 2.2: Factorization of D_m

The factorization of D_5 almost contains all the primes up to $2^5 = 32$. Only 23 is missing. The reason is that we have

$$\begin{aligned} \mathrm{ord}_{23}(2) &= 11, \\ \mathrm{ord}_{11}(2) &= 10, \\ \mathrm{ord}_{5}(2) &= 4. \end{aligned}$$

In order to have $23 \mid D_m$, $23 \,\Big|\, 2^{D_{m-1}} - 1$ by equation 2.4, which implies $11 \mid D_{m-1}$. Similarly, $11 \,\Big|\, 2^{D_{m-2}} - 1$ by equation 2.4. Then, $10 \mid D_{m-2}$. $10 = 2 \cdot 5$ implies $2 \mid E_{m-3}$ and $5 \,\Big|\, 2^{D_{m-3}} - 1$. Then, $4 \mid D_{m-3}$, which implies $4 \mid E_{m-4}$ and $m - 4 \geq 2$. Therefore, $m \geq 6$.

2.1.3 Sophie-Germain primes

A positive integer p is a Sophie-Germain prime if both p and $2p+1$ are primes. Since $\mathrm{ord}_{2p+1}(2) \neq 2$ for Sophie-Germain prime p, $\mathrm{ord}_{2p+1}(2) = p$ or $\mathrm{ord}_{2p+1}(2) = 2p$. If $p \nmid D_k$, $2p+1 \nmid 2^{D_k} - 1$, which implies $2p+1 \nmid D_{k+1}$. This idea is used to prove theorem 2.4 below.

Definition 2.3. *A sequence of primes, $p_1, p_2, \cdots, p_n$, is called a Sophie-Germain chain if $p_{k+1} = 2p_k + 1$ for $k = 1, 2, \cdots, n-1$.*

Theorem 2.4. *Let $p_1, p_2, \cdots, p_n$ be a Sophie-Germain chain. For $m > 2$, $p_1 \mid D_m$ if and only if $p_n \mid D_{m+n-1}$.*

Proof. It is enough to show the case $n = 2$. Then, the theorem follows by induction.

It is obvious that $4 \mid D_m$ for $m > 2$. If $p_1 \mid D_m$, $D_m = 2p_1 t$ for some integer t. Then,

$$\begin{aligned} D_{m+1} &= E_m(2^{D_m} - 1) \\ &= E_m(2^{2p_1 t} - 1) \\ &= E_m(2^{2p_1} - 1)(2^{2p_1(t-1)} + 2^{2p_1(t-2)} + \cdots + 1). \end{aligned}$$

$\mathrm{ord}_{p_2}(2)$ divides $\phi(p_2) = 2p_1$. Therefore, $2^{2p_1} \equiv 1 \pmod{p_2}$ and $p_2 \mid D_{m+1}$.

If $p_2 \mid D_{m+1}$, then $p_2 \mid 2^{D_m} - 1$. $\mathrm{ord}_{p_2}(2)$ divides D_m. For being a Sophie-Germain chain, $p_2 \geq 5$. $\mathrm{ord}_{p_2}(2) > 2$ since $2^2 = 4 < 5$. $\mathrm{ord}_{p_2}(2)$ divides $\phi(p_2) = 2p_1$. Then, p_1 divides $\mathrm{ord}_{p_2}(2)$. Hence, p_1 divides D_m. $\square$

Remark: The theorem does not apply to the case $m = 2$. It is because $D_2 = 2$, which cannot be written as $2p_1 t$ when $p_1 = 2$.

For example, the sequence $5, 11, 23$ is a Sophie-Germain chain. $5 \nmid D_3$ implies $23 \nmid D_5$ by theorem 2.4.

2.2 Divisibility of $D_{r,m}$ with r odd

In this section, we consider $D_{r,k}$ for positive odd r. If $r = 1$, $D_{1,k} = 0$ for all $k > 0$. It is a degenerate case. Table 2.3 and 2.4 show the factorizations of some $D_{3,k}$ and $D_{5,k}$. Note that all 2-bit numbers divide both $D_{3,2}$ and $D_{5,2}$, all 3-bit numbers divide both $D_{3,3}$ and $D_{5,3}$. For $D_{5,3}$, even all 4-bit numbers divide it.

k	$E_{3,k}$	$D_{3,k}$	Factorization of $D_{3,k}$
0	1	1	1
1	3	2	2
2	27	24	$2^3 \cdot 3$
3	7625597484987	7625597484960	$2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 41 \cdot 73 \cdot 6481$

Table 2.3: Factorization of $D_{3,k}$

k	$E_{5,k}$	$D_{5,k}$	Factorization of $D_{5,k}$
0	1	1	1
1	5	4	2^2
2	3125	3120	$2^4 \cdot 3 \cdot 5 \cdot 13$
3	5^{3125}	$5^{3125} - 3125$	$2^6 \cdot 3^2 \cdot 5^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 31 \cdot 41 \cdots$

Table 2.4: Factorization of $D_{5,k}$

The results given in this section usually are one step better than the case of r even. It is because $D_{r,1} = r-1$ is even, which provides 2 as a factor for the later values in the sequence. We show a divisibility theorem which tells that $D_{r,m}$ is divisible up to $2^m - 1$. Before presenting the theorem, we show there are enough factors of 2 in each $D_{r,m}$.

Proposition 2.5. *For r odd, $r > 1$ and $m > 0$, if $2^k \mid D_{r,m}$, then $2^{k+2} \mid D_{r,m+1}$.*

Proof. Since $D_{r,m} \mid D_{r,m+1}$ by proposition 2.1, the statement is equivalent to

$$4D_{r,m} \text{ divides } D_{r,m+1} \text{ for } m > 0.$$

We prove it by induction.

For the base case, if $r \equiv 1 \pmod 4$, 4 divides $r - 1 = D_{r,1}$. Then $4D_{r,0} = 4$ divides $D_{r,1}$. If $r \equiv 3 \pmod 4$, $D_{r,1} = r - 1 \equiv 2 \pmod 4$ and

$$\begin{aligned} D_{r,2} &= r(r^{r-1} - 1) \\ &\equiv r(r^{\frac{r-1}{2}} - 1)(r^{\frac{r-1}{2}} + 1) \\ &\equiv 0 \pmod 8. \end{aligned}$$

Therefore, $4D_{r,1}$ divides $D_{r,2}$.

Assume $4D_{r,m-1}$ divides $D_{r,m}$ for some $m > 1$. Write $D_{r,m} = 2^k t$ with t odd and $k \geq 2$. $E_{r,m-1}(r^{D_{r,m-1}} - 1) = D_{r,m} \equiv 0 \pmod{2^k}$. Since $E_{r,m-1}$ is odd, $r^{D_{r,m-1}} \equiv s2^k + 1 \pmod{2^{k+2}}$, where $s = 0, 1, 2$ or 3.

$$\begin{aligned} r^{4D_{r,m-1}} &\equiv (s2^k + 1)^4 \\ &\equiv s^4 2^{4k} + 4s^3 2^{3k} + 6s^2 2^{2k} + 4s2^k + 1 \\ &\equiv 1 \pmod{2^{k+2}}. \end{aligned}$$

Then, $D_{r,m+1} = E_{r,m}(r^{D_{r,m}} - 1) \equiv 0 \pmod{2^{k+2}}$. □

Corollary 2.6. *For $r > 1$ and $k > 0$, if $r \equiv 1 \pmod 4$, $2^{2k} \mid D_{r,k}$. For $r \equiv 3 \pmod 4$, $2^{2k-1} \mid D_{r,k}$.*

Proof. We prove it by induction. $4 \mid r - 1$ if $r \equiv 1 \pmod 4$. $2 \mid r - 1$ if $r \equiv 3 \pmod 4$. The base cases are true. The induction step follows from proposition 2.5. □

Theorem 2.7. *Let r be a positive odd integer. For any $n \in \mathbb{N}$, if $n < 2^m$, then $n \mid D_{r,m}$.*

Proof. We prove it by showing it satisfies all the hypotheses in proposition 2.2 for $b = 2$. Then, the theorem follows.

For hypothesis (i), $D_{r,2} = r(r^{r-1} - 1)$ is divisible by 2 since $r^{r-1} - 1$ is divisible by 2. If $r \equiv 0 \pmod 3$, $3 \mid D_{r,2}$. Otherwise, $\mathrm{ord}_3(r) = 1$ or $\mathrm{ord}_3(r) = 2$ imply $\mathrm{ord}_3(r) \mid r - 1$, which further implies $3 \mid r^{r-1} - 1$. Therefore, 6 divides $D_{r,2}$.

For hypothesis (ii), if a is even, $\phi(a) \leq \frac{a}{2} < 2^k$, then $\phi(a) \mid D_{r,k}$ by the assumption given in (ii). For odd a, $\phi(a) = 2^u v$ with $0 < u \leq k$, v odd and $v < 2^k$. $2^u \mid D_{r,k}$ since $2^k \mid D_{r,k}$ by corollary 2.6. $v \mid D_{r,k}$ by the assumption in (ii). Therefore, $\phi(a)$ divides $D_{r,k}$. $\square$

2.3 Divisibility of $D_{r,m}$ with r even

In this section, we prove the divisibility theorem when r is even. Table 2.5 and 2.6 show some factorizations of $D_{4,k}$ and $D_{6,k}$. Note that $D_{r,1} = r - 1$ must be odd. For $r > 2$, 2 is not the smallest prime dividing the first $D_{r,k} > 1$. We show $D_{r,m}$ is divisible up to $2^m - 1$. Like the proof of theorem 2.7, we prove the hypotheses of proposition 2.2 for $b = 3$ can be satisfied.

k	$E_{4,k}$	$D_{4,k}$	Factorization of $D_{4,k}$
0	1	1	1
1	4	3	3
2	256	252	$2^2 \cdot 3^2 \cdot 7$
3	4^{256}	$4^{256} - 256$	$2^8 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 37 \cdot 43 \cdot 73 \cdots$

Table 2.5: Factorization of $D_{4,k}$

k	$E_{6,k}$	$D_{6,k}$	Factorization of $D_{6,k}$
0	1	1	1
1	6	5	5
2	46656	46650	$2 \cdot 3 \cdot 5^2 \cdot 311$
3	6^{46656}	$6^{46656} - 46656$	$2^6 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 31 \cdot 43 \cdot 101 \cdots$

Table 2.6: Factorization of $D_{6,k}$

Theorem 2.8. *Let $r > 2$ be a even integer. For any $n \in \mathbb{N}$, if $n < 2^m$, then $n \mid D_{r,m+1}$.*

Proof. For hypothesis (i), $D_{r,3} = r^r(r^{r^r-r}-1)$. $2 \mid D_{r,3}$ since r is even. If $r \equiv 0 \pmod 3$, $3 \mid r^r$. Otherwise, $r^2 \equiv 1 \pmod 3$. Then, $(r^2)^{\frac{r}{2}(r^{r-1}-1)} \equiv 1 \pmod 3$ and $3 \,\big|\, r^{r^r-r}-1$. Therefore, $3 \mid D_{r,3}$.

For hypothesis (ii), a is odd since r is even. $\phi(a) = 2^u v$ with $0 < u \leq k$, v odd and $v < 2^k$. $2^u \mid D_{r,k+1}$ since, obviously, $2^k \,\big|\, D_{r,k+1}$. $v \mid D_{r,k+1}$ by the assumption in hypothesis (ii). Therefore, $\phi(n)$ divides $D_{r,k+1}$.

The theorem follows from proposition 2.2 with $b = 3$. □

2.4 Convergence of $r^{r^{r^{\cdot^{\cdot^{\cdot}}}}} \pmod p$

In [3], Ng showed by p-adic valuation that, for any prime p and any positive integer r, $\lim_{k\to\infty} E_{r,k} \pmod p$ exists. We use a different technique to prove a more general result, $\lim_{k\to\infty} E_{r,k} \pmod n$ exists for any $n > 1$, and even evaluate the limit. We begin with a unified version of the divisibility theorem. Then, we show that $E_{r,k} \pmod n$ stabilizes for large k. At last, the limit is evaluated.

Theorem 2.9. *Let n be a positive integer with $n < 2^m$. Then, $n \mid D_{r,m+1}$ for any positive integer r.*

Proof. For $r = 1$, it is trivial. For the other cases, it follows by theorem 2.7 and 2.8. □

Proposition 2.10. *Let n be an integer with $1 < n < 2^m$ and r be a positive integer. Then, for any $k \geq m$,*

$$E_{r,k} \equiv E_{r,m} \pmod n. \tag{2.8}$$

Proof. n divides $D_{r,m+1}$ by theorem 2.9. Then, by proposition 2.1, n divides $D_{r,j}$ for $j > m+1$. Hence, we have $E_{r,k} = \sum_{j=m+2}^{k} D_{r,j} + E_{r,m+1} \equiv E_{r,m+1} \pmod n$. The proposition follows. □

Theorem 2.11. *Let n be an integer with $1 < n < 2^m$ and r be a positive integer.*

$$\lim_{k\to\infty} E_{r,k} \equiv E_{r,m} \pmod n \tag{2.9}$$

Proof. For $h \geq 0$, $E_{r,m+h} \equiv E_{r,m} \pmod n$ by proposition 2.10. Then,

$$\lim_{k\to\infty} E_{r,k} = \lim_{h\to\infty} E_{r,m+h} \equiv \lim_{h\to\infty} E_{r,m} = E_{r,m} \pmod n.$$

□

We will discuss how to compute $E_{r,m} \pmod n$ in section 3.1.

2.5 Partitionings of prime numbers

For $k > 0$, define subsets of prime numbers

$$\mathcal{P}_{r,k} \quad = \quad \{p \ : \ p \text{ prime}, p \mid D_{r,k} \ \text{ and } p \nmid D_{r,k-1}\}\,. \tag{2.10}$$

Then, for $r > 0$, $\mathcal{P}_{r,1}, \mathcal{P}_{r,2}, \mathcal{P}_{r,3}, \cdots$ is a partitioning of all prime numbers. With Birkhoff and Vandiver's theorem (proposition 2.12), we can show $\mathcal{P}_{r,k}$ is non-empty for $r > 1$ and $k > 0$, except the trivial case $\mathcal{P}_{2,1}$. Hence, we have a non-empty partitioning of primes for each $r > 2$.

Proposition 2.12. *Let $V_n = a^n - b^n$ for some integers a, b with $a > b > 0$ and $\gcd(a, b) = 1$. If $n \neq 2$ and $V_n \neq 2^6 - 1^6$, then there exists a prime p, such that $p \mid V_n$ and $\gcd(p, V_d) = 1$ for all $d \mid n$ and $d < n$.*

See [1] for the proof of proposition 2.12.

Theorem 2.13. *$\{\mathcal{P}_{2,k}\}_{k>1}$ and $\{\mathcal{P}_{r,k}\}_{k>0}$ for $r > 2$ are non-empty partitionings of primes.*

Proof. For any $r > 1$ and any prime p with $p < 2^m$, p does not divide $D_{r,0} = 1$ and p divides $D_{r,m+1}$ by theorem 2.9. Therefore, $p \in \mathcal{P}_{r,k}$ for some $0 < k \leq m + 1$. Since $D_{r,a} \mid D_{r,b}$ for all $a < b$ by proposition 2.1, $p \notin \mathcal{P}_{r,h}$ for $h \neq k$. Therefore, $\{\mathcal{P}_{r,k}\}_{k>0}$ is a partitioning of primes.

$\mathcal{P}_{2,2} = \{2\}$ and $\mathcal{P}_{2,3} = \{3\}$ are non-empty. Let

$$I = \left\{(r, k) \in \mathbb{N}^2 \ : \ k > 3 \text{ if } r = 2 \text{ and } k > 1, \text{ otherwise.}\right\}.$$

We show $\mathcal{P}_{r,k}$ is non-empty for $(r, k) \in I$. For any $r > 1$ and $k > 1$, $D_{r,k-1} \neq 2$. For $k > 3$, $D_{2,k-1} \neq 6$. By propostion 2.12, for $(r, k) \in I$, there exists a prime q, such that $q \mid r^{D_{r,k-1}} - 1^{D_{r,k-1}}$ and $q \nmid r^d - 1^d$ for $d \mid D_{r,k-1}$ and $d < D_{r,k-1}$. $D_{r,k-2} \mid D_{r,k-1}$ and $D_{r,k-2} < D_{r,k-1}$ imply $q \nmid r^{D_{r,k-2}} - 1^{D_{r,k-2}}$. $q \nmid E_{r,k-2}$ since $q \mid r^{D_{r,k-1}} - 1$. Therefore, q divides $D_{r,k} = E_{r,k-1}(r^{D_{r,k-1}} - 1^{D_{r,k-1}})$, but not $D_{r,k-1} = E_{r,k-2}(r^{D_{r,k-2}} - 1^{D_{r,k-2}})$. $\mathcal{P}_{r,k}$ is non-empty. □

2.5.1 Height function

It is natural to ask that given $r > 1$ and a prime p, how to find k, such that $p \in \mathcal{P}_{r,k}$? i.e. which partition p belongs to?

Definition 2.14. *For $r > 1$, define the height function,*

$$h_r : \mathbb{P} \to \mathbb{N}, \qquad p \mapsto k, \tag{2.11}$$

such that $p \in \mathcal{P}_{r,k}$, where $\mathbb{P}$ is the set of primes.

The problem is equivalent to finding the minimum k, such that p divides $D_{r,k}$ because $p \nmid D_{r,j}$ for $j < h_r(p)$ and $p \mid D_{r,j}$ for $j \geq h_r(p)$. Definition 2.14 can be extended to any $n > 1$ as below.

Definition 2.15. *For $r > 1$, define the height function,*

$$h_r : \mathbb{N} \setminus \{1\} \to \mathbb{N}, \qquad n \mapsto k, \tag{2.12}$$

such that $n \mid D_{r,k}$ and $n \nmid D_{r,k-1}$.

Suppose $n < 2^m$. $h_r(n)$ can be computed by a binary search algorithm since $h_r(n) \leq m + 1$ by theorem 2.9.

Algorithm 2.16. heightByBinarySearch(r, n)

```
{
    set lower = 0;
    set upper = m + 1;
    while true
    {
        if upper − lower = 1, return upper;
        set mid = ½(upper + lower);
        if n | D_{r,mid}
            upper = mid;
        else
            lower = mid;
    }
}
```

The number of loops required before returning is $O(\log \log p)$. However, $p \mid D_{r,j}$ may not be determined efficiently for $j \leq m$ because $D_{r,j}$ can be much larger than p. We present another algorithm, heightByOrd, which does not query whether $p \mid D_{r,j}$, except for small j. From the example at the end of section 2.1.2, it suggests the following algorithm.

Algorithm 2.17. heightByOrd(r, n)

```
{
    if n | D_{r,1}, return 1;
    if n | D_{r,2}, return 2;
    write n = st for s, t ≥ 1, each prime divisor of s divides r and gcd(r, t) = 1;
    find a = min {j : s | E_{r,j}};
    find d = ord_t(r);
    return max(a, heightByOrd(r, d) + 1);
}
```

The number of recursion steps in heightByOrd is $O(h_r(n))$. Since $h_r(n) < \log_2 n + 2$ by theorem 2.9, the number of recursions is $O(\log n)$.

The algorithm requires computing $\mathrm{ord}_t(r)$, where $\mathrm{ord}_t(r)$ can be computed efficiently if the factorization of t can be computed efficiently. We will further discuss the factoring problem in section 3.

3 Factoring

We show that the factoring problem, denoted by FACTOR, is closely related to the problem of computing $D_{r,k} \bmod n$, where the operation, $\bmod n$, returns the remainder of $D_{r,k}$ divided by n, which is a non-negative integer less than n. These two problems are probably equivalent. Thoughout this section, n is an m-bit number greater than 1.

3.1 Computing $D_{r,k} \bmod n$

Computing $D_{r,k} \bmod n$ in general is difficult since $D_{r,k}$ can be huge for $k \in O(\log n)$. The problem of computing $D_{r,k} \bmod n$ is denoted by DMOD and, similarly, the problem of computing $E_{r,k} \bmod n$ is denoted by EMOD. We only consider $1 < r < n < 2^m$ and $k \geq 0$. We first show that DMOD and EMOD are polynomial-time equivalent. Then, we present an algorithm for EMOD.

Proposition 3.1. DMOD *and* EMOD *are polynomial-time, in* $\log n$*, equivalent.*

Proof. Given an algorithm solving EMOD, DMOD can be solved by,

$$D_{r,k} \bmod n = ((E_{r,k} \bmod n) - (E_{r,k-1} \bmod n)) \bmod n.$$

On the other hand, given an algorithm solving DMOD, EMOD can be solved as following. If $k < m + 1$,

$$E_{r,k} \bmod n = \left(\sum_{j=0}^{k} (D_{r,j} \bmod n) \right) \bmod n. \tag{3.13}$$

Otherwise, $k \geq m + 1$, by proposition 2.10,

$$E_{r,k} \bmod n = E_{r,m} \bmod n,$$

which can be computed by equation (3.13).

Obviously, both transformations require $O(\log n)$ steps. □

Algorithm 3.2. EMod(r, k, n)

{
    if $k \geq m+1$, return $\mathsf{EMod}(r, m, n)$;

    write $n = st$ for $s, t \geq 1$, each prime divisor of s divides r and $\gcd(r, t) = 1$;
    if $t = 1$, return $E_{r,k} \bmod s$;

    set $d = \mathrm{ord}_t(r)$;
    set $h = \mathsf{EMod}(r, k-1, d)$;
    return $(s^{-1}r^h \bmod t)s$;
}

Computing $\mathrm{ord}_t(r)$ turns out to require factoring t. For $E_{r,k} \bmod s$, if k is small, it can be computed directly, otherwise, $E_{r,k} \bmod s = 0$. All other steps can be computed efficiently.

3.2 A factoring algorithm

We present a deterministic algorithm for factoring n, where n is a composite, m-bit number.

Algorithm 3.3. $\mathsf{factor}(n)$

{
    for $r = 2$ to $\lfloor\sqrt{n}\rfloor + 1$
        for $k = 1$ to m
        {
            set $h = D_{r,k} \bmod n$;
            set $d = \gcd(h, n)$;
            if $d \neq 1$ and $d \neq n$
                return d;
        }
}

Proposition 3.4. *Let p, q be distinct prime factors of n. If there exists $r_0 \leq \lfloor\sqrt{n}\rfloor + 1$, such that $h_{r_0}(p) < h_{r_0}(q)$, then* factor *returns at $r \leq r_0$.*

Proof. Note that $D_{r,k} \bmod n = 0$ for $k > m$ by theorem 2.9. Therefore, $h_{r_0}(q) \leq m$. Let $k_0 = h_{r_0}(p)$. $D_{r_0,k_0} = pt$ for some integer t. $\gcd(q, t) = 1$ since $q \not| D_{r_0,k_0}$. Then, $D_{r_0,k_0} \bmod n = ps$ for some integer s with $\gcd(q, s) = 1$. Therefore, $\gcd(D_{r_0,k_0}, n)$ is not equal to 1 or n. The algorithm returns at $r \leq r_0$. □

Proposition 3.5. *If n is composite,* $\mathsf{factor}(n)$ *returns a non-trivial factor of n.*

Proof. Clearly, if factor returns, it returns a non-trivial divisor of n. There exists a prime p, such that $p \mid n$ and $p < \lfloor\sqrt{n}\rfloor + 1$. Let $r_0 = p + 1$ and $k_0 = 1$. Then, $D_{r_0,k_0} = p$. factor returns at $r \leq r_0$. □

Suppose $n = pq$, where p, q are distinct primes with $p < q$. factor is not an interesting algorithm if it returns at $r = p+1$, since a naive factoring algorithm, which checks each prime for divisor of n in ascending order, has similar property. We hope that there is an r in $O(\log n)$, such that factor returns. It is the case if conjecture 3.6 below is ture. As a consequence, Factor and DMod are polynomial-time equivalent.

For example, in The New RSA Factoring Challenge [2], RSA-160 = PQ, where

$$\begin{aligned} P &= 45427892858481394071686190649738831656137145778469793 \\ &\quad 25095998470925000415733 5359, \\ Q &= 4738809060383201619663383230378895197326892292104095 \\ &\quad 7944741354648812028493909367. \end{aligned}$$

We have $h_2(P) = 12$ and $h_2(Q) = 11$. Therefore, factor will return Q, although $Q > P$, when $r = 2$ and $k = 11$ in algorithm 3.3.

Conjecture 3.6. *For any distinct primes p, q, there exists an r in $O(\log p + \log q)$, such that $h_r(p) \neq h_r(q)$.*

Theorem 3.7. *If conjecture 3.6 is true,* Factor *and* DMod *are polynomial-time, in* $\log n$*, equivalent.*

Proof. Given an algorithm solving DMod in polynomial-time, algorithm 3.3 solves Factor in polynomial-time if conjecture 3.6 is true.

On the other hand, given an algorithm solving Factor in polynomial-time, algorithm 3.2 solves EMod in polynomial-time. By proposition 3.1, DMod can be solved in polynomial-time. □

References

[1] G. D. Birkhoff and H.S. Vandiver. On the integral divisors of $a^n - b^n$. *The Annals of Mathematics*, 5(4):173–180, July 1904.

[2] RSA Security Inc. The new rsa factoring challenge. RSA-160 is factored! (`http://www.rsasecurity.com/rsalabs/node.asp?id=2097`), 2003.

[3] L. L. Ng. A problem in p-adics, 1989.

[4] N. J. A. Sloane. Sequences a038081 and a014221. The On-Line Encyclopedia of Integer Sequences (`http://www.research.att.com/~njas/sequences/Seis.html`).