23.02.

1 Pollard's ρ-method

Let $N \in \mathbb{N}$ and $p \mid N$. We say that $f : \mathbb{Z}_N \to \mathbb{Z}_N$ is *compatible with* $\bmod p$ if $f((a) \bmod p) \equiv f(a) \pmod p$ for each $a \in \mathbb{Z}_N$.

1.1. Let $N \in \mathbb{N}$, $p \mid N$ and $g \in Z_N[x]$. Show that if $f : \mathbb{Z}_N \to \mathbb{Z}_N$ is defined by $f(a) = g(a)$ for each $a \in \mathbb{Z}_N$, then f is compatible with $\bmod p$.

It is an easy inductive consequence of the definition and the fact that

$$(a) \bmod p \equiv a \pmod p.$$

□

1.2. Compute the period and preperiod of the sequence $\{s_n\}_{n\geq 0}$ given by the affine mapping $f(x) = ax + b \in \mathbb{Z}_p$ for $x \in \mathbb{Z}_p$, where $p \in \mathbb{P}$, i.e. $s_0 \in \mathbb{Z}_p$ and $s_{n+1} = f(s_n)$, if

(a) $a = 1$, $b \in \mathbb{Z}_p$,

(b) $a \in \mathbb{Z}_p^*$, $b = 0$.

(a) First we express directly the non-recursive formula $s_n = s_0 + nb$.

If $b = 0$, then the sequence is constant and therefore has a preperiod of $m = 0$ and a period of $t = 1$.

If $b \neq 0$, we have $ib \neq 0$ for $i = 1, \ldots, p-1$ and $pb = 0$, which means $m = 0$ is the preperiod and a $t = p$ is a period of $\{s_n\}_{n\geq 0}$.

(b) Again, it is easy to determine the non-reciprocal formula $s_n = a^n s_0$.

If $s_0 = 0$, the sequence is constant, i.e. the sequence with preperiod $m = 0$ and period $t = 1$.

If $s_0 \neq 0$, we see that the preperiod of the sequence is zero, since $a^{p-1} = 1$ and that the smallest natural number is t satisfying $s_0 = s_0 a^t$, i.e. the period of the sequence, is equal to the order $t = o_{\mathbb{Z}_p^*}(a)$. □

1.3. Let p be a safe prime number, i.e. there exists prime q such that $p = 2q + 1$. Determine all $a \in \mathbb{Z}_p^*$ for which the period of $\{s_n\}_{n\geq 0}$ from 1.2(b) is less then q

Since the group $\mathbb{Z}_p^*$ is cyclic of the order $p-1 = 2q$, it contains exactly one element $a = 1$ of order 1 and exactly one element $a = -1$ of order 2. Then $\mathbb{Z}_p^*$ contains $(q-1)$ elements of order q, and the same number of elements of order $2q$. By 1.2(b) the period of $\{s_n\}_{n\geq 0}$ is less then q if and only if $a = \pm 1$. □

Observe that 1.2 shows that the walk through the different numbers of the sequence in Pollard's algorithms would is too long.

1.4. Let us denote $f_{a,b} : \mathbb{Z}_p \to \mathbb{Z}_p$ affine transformation given by the rule $f_{a,b}(x) = ax + b$ and put $\mathrm{Aff}(\mathbb{Z}_p) = \{f_{a,b} \mid a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p\}$. Show $\mathrm{Aff}(\mathbb{Z}_p)$ is a subgroup of the symmetric group $S(\mathbb{Z}_p)$ for $p \in \mathbb{P}$ and determine computational rules for operations of the group $\mathrm{Aff}(\mathbb{Z}_p)$.

First, observe that $f_{a,b}$ is an injective operator on the finite set, hence is is a bijection. Furtheremore, it is clear that $f_{1,0} = \mathrm{id}$ and that

$$f_{a,b}f_{c,d}(x) = a(cx + d) + b = acx + ad + b = f_{ac,ad+b}(x).$$

hence $f_{a,b}f_{c,d} = f_{ac,ad+b}$. Finally, we can directly calculate that

$$f_{a,b} \circ f_{a^{-1},-a^{-1}b} = f_{1,0} = \mathrm{id},$$

hence $f_{a,b}^{-1} = f_{a^{-1},-a^{-1}b}$. Form it follows that $\mathrm{Aff}(\mathbb{Z}_p)$ is closed under compositions and inversions and so it is a subgroup of $S(\mathbb{Z}_p)$. □

1.5. Compute the period and preperiod of the sequence $\{s_n\}_{n\geq 0}$ given by the polynomial mapping $f : \mathbb{Z}_p \to \mathbb{Z}_p$ for $p \in \mathbb{P}$, if

(a) $f(x) = ax + b$, $a, b \in \mathbb{Z}_p^*$ and $a \neq 1$.

(b) $f(x) = x^2$.

(a) Using the previous task, we find c so that $f_{1,c}f_{a,b}f_{1,c}^{-1} = f_{u,0}$. First we calculate

$$f_{1,c}f_{a,b}f_{1,c}^{-1} = f_{1,c}f_{a,b}f_{1,-c} = f_{a,b+c}f_{1,-c} = f_{a,-ac+b+c},$$

then the condition $-ac + b + c = 0$ implies that $c = b(a-1)^{-1}$.

Let us denote $g = f_{1,c}$, $f = f_{a,b}$ and $h = gfg^{-1}$. Since $s_n = f^n(s_0) = g^{-1}h^n(g(s_0))$, we see that $s_i = s_j$ if and only if $h^i(g(s_0)) = h^j(g(s_0))$. Hence the period and preperiod of the sequences $\{s_n\}_{n\geq 0}$ and $\{h^n(g(s_0))\}_{n\geq 0}$ are the same. Now it remains to use 1.2, which says that for $s_0 = -c$, both sequences are constant, i.e. they have a preperiod $m = 0$ and a period $t = 1$, and for $s_0 \neq -c$, both sequences have a preperiod of $m = 0$ and a period of $t = o_{\mathbb{Z}_p^*}(a)$.

(b) First, we observe that the recurrent formula $s_{n+1} = s_n^2$ immediately implies the non-recurrent formula $s_n = s_0^{2^n}$. We also note that for s_0 equal to 0 or 1, the sequence is constant, i.e. it has the preperiod 0 and the period 1.

Let $s_0 \neq 0, 1$. Then we can thus limit ourselves to looking for the smallest i and the smallest $j > i$, for which it is true that $s_i = s_j$. If we find such i, j, then i is the preperiod and $j - i$ the period of the sequence. Consider a number of equivalent conditions in the $\mathbb{Z}_p^*$group

$$s_i = s_j \Leftrightarrow s_0^{2^i} = s_0^{2^j} \Leftrightarrow s_0^{2^j - 2^i} = 1 \Leftrightarrow s_0^{2^i(2^{j-i}-1)} = 1 \Leftrightarrow o_{\mathbb{Z}_p^*}(s_0) \mid 2^i(2^{j-i} - 1),$$

where the last equivalence follows from the fact that an exponent of the element is precisely the multiple of the order of the element. Now we express $o_{\mathbb{Z}_p^*}(s_0) = 2^e l$ using $e = v_2(o_{\mathbb{Z}_p^*}(s_0))$, where l is odd. Then we get the equivalences

$$o_{\mathbb{Z}_p^*}(s_0) \mid 2^i(2^{j-i} - 1) \Leftrightarrow i \geq e,\ l \mid 2^{j-i} \Leftrightarrow i \geq e,\ 2^{j-i} \equiv 1 \pmod{l}.$$

The minimum values are achieved for the preperiod $m = i = e$ and the period $t = j - i = o_{\mathbb{Z}_l^*}(2)$. □

2 B-powersmooth numbers

2.1. Determine the value of e_B and calculate all numbers that are B-powersmooth, if (a) $B = 4$, (b) $B = 10$.

(a) We see that the prime numbers $2, 3$ are less than or equal to 4, hence

$$e_4 = 2^{\lfloor \log_2(4) \rfloor} 3^{\lfloor \log_3(4) \rfloor} = 2^2 \cdot 3^1 = 12.$$

We know from the lecture that B-powersmooth numbers divide e_B, and we can easily see that every divisor of e_B is a B-powersmooth number. Therefore, the set $\{2^i \cdot 3^j \mid i \in \mathbb{Z}_3, j \in \mathbb{Z}_2\}$ contains all 4-powersmooth numbers, of which there are $3 \cdot 2 = 6$.

(b) As in (a), we can see that only the prime numbers $2, 3, 5, 7 \leq 10$ and

$$e_{10} = 2^{\lfloor \log_2(10) \rfloor} 3^{\lfloor \log_3(10) \rfloor} 5^{\lfloor \log_5(10) \rfloor} 7^{\lfloor \log_7(10) \rfloor} = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520.$$

Furthermore, the set of all 10-power numbers $\{2^i \cdot 3^j \cdot 5^k \cdot 7^l \mid i \in \mathbb{Z}_4, j \in \mathbb{Z}_3, k, l \in \mathbb{Z}_2\}$ contains $48 = 4 \cdot 3 \cdot 2^2$ different values. □

2.2. For (a) $B = 4$, (b) $B = 10$, find all prime numbers $p \leq 20$ for which the B-powersmooth are $p - 1$.

(a) We are looking for prime numbers $p \leq 20$ for which $p - 1 \mid 12$. We see that these are precisely the prime numbers

$$1 + 1 = 2,\ 2 + 1 = 3,\ 4 + 1 = 5,\ 6 + 1 = 7,\ 12 + 1 = 13.$$

(b) In addition to all the values from (a), we also have the prime numbers

$$10 + 1 = 11,\ 18 + 1 = 19,$$

thus the list of such prime contains exactly: $2, 3, 5, 7, 11, 19$ □

2.3. If p is a safe prime such that $p - 1$ is B-powersmooth. Find a lower bound of B.

Since p is safe, there exists $\tilde{p}$ such that $p = 2\tilde{p} + 1$. Thus $p - 1 = 2\tilde{p}$, hence $B \geq \tilde{p} = \frac{p-1}{2}$. □

The previous task shows that for $N = pq$, where p, q are safe primes with close lengths, the Pollard p-1 method is not efficient way to find a proper divisor.

Recall that the number $F_n = 2^{2^n} + 1$ is called a *Fermat number*, obviously $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ are prime numbers.

2.4. Prove that F_4 is a prime number.

Since $F_4 - 1 = 2^{16} \equiv -1 \pmod{F_4}$, it is easy to see that the prime divisor $p > 2$ of the number F_4 satisfies the congruence

$$2^{16} \equiv -1 \pmod{p} \quad \text{and} \quad 2^{32} \equiv 1 \pmod{p},$$

which means that the order of the element 2 in the group $\mathbb{Z}_p^*$ is exactly 32. Lagrange theorem also implies that every element of the group $\mathbb{Z}_p^*$ is of the exponent $p - 1$, hence $32 \mid p - 1$. This means that $p = 32k + 1$ for some k. Any proper divisor of the number F_4 must be at most $\sqrt{F_4} < 2^8 + 1 = F_3 = 257$, so it suffices to consider the prime numbers from the values $32k + 1$ for $k = 1, \ldots 7$, which, as we can easily calculate, are only the values 97 and 193. For both, we can directly check by standard division that both are not divisors of the number F_4. Thus F_4 is a prime number. □

2.5. Use an appropriate variant of Pollard's $p - 1$-method to show that F_5 is composite.

Since we know the prime factor 641 of the number F_5, we can see that $641-1 = 2^7 \cdot 5$ is the exponent of every element $\mathbb{Z}^*_{641}$, i.e., $a^{640} \equiv 1 \pmod{641}$ for every $a \in \mathbb{Z}^*_{F_5}$. So we choose the value $B = 2^7 = 128$ and modify the second variant of Pollard's $p-1$-method so that instead of the value e_{128}, which works with the product of too many numbers, we consider the value $\hat{e}_{128} = 2^7 \cdot 3^4 \cdot 5^3$, about which we know that $640 \mid \hat{e}_{128}$.

At the same time, let us remember that $2^{64} \equiv 1 \pmod{F_5}$, which means that

$$2^{\hat{e}_{128}} \equiv (2^{64})^{2 \cdot 81 \cdot 125} \equiv 1 \pmod{F_4}.$$

Since $2^{\hat{e}_{128}} \equiv 1 \pmod{640}$, we have $\gcd(2^{\hat{e}_{128}} - 1, F_5) = F_5$, so using $a = 2$ we cannot find a prime divisor of 641. Therefore, we choose $a = 3$ and calculate

$$a_1 = (3^{81}) \bmod F_5 = 1918862017, \quad a_2 = (a_1^{125}) \bmod F_5 = 4292273029.$$

Now we will test the greatest common divisors $\gcd(a_i - 1, F_5)$ and calculate $a_{i+1} = (a_i^2) \bmod F_5$:

$$\gcd(a_2 - 1, F_5) = 1, \quad a_3 = (a_2^2) \bmod F_5 = 585323894,$$

$$\gcd(a_3 - 1, F_5) = 1, \quad a_4 = (a_3^2) \bmod F_5 = 4278871505,$$
$$\gcd(a_4 - 1, F_5) = 1, \quad a_5 = (a_4^2) \bmod F_5 = 2092752224,$$
$$\gcd(a_5 - 1, F_5) = 1, \quad a_6 = (a_5^2) \bmod F_5 = 2812764726,$$
$$\gcd(a_6 - 1, F_5) = 1, \quad a_7 = (a_6^2) \bmod F_5 = 1314231249,$$
$$\gcd(a_7 - 1, F_5) = 1, \quad a_8 = (a_7^2) \bmod F_5 = 3257626099,$$
$$\gcd(a_8 - 1, F_5) = 1, \quad a_9 = (a_8^2) \bmod F_5 = 3616864936.$$

Now we get that $\gcd(3^{\hat{e}_{128}} - 1, F_5) = \gcd(a_9 - 1, F_5) = 641$, which verifies that F_5 is a composite number. □

23.03.

2.6. Let $p > 5$ be a safe prime number, i.e. there exists a prime number q satisfying $p = 2q + 1$. Prove that $p + 2$ is not a safe prime.

Since $p > 5$, q is odd prime and so $p + 2 = 2(q + 1) + 1$ where $q + 1 > 2$ is even, hence q is not prime. □

2.7. For (a) $B = 4$, (b) $B = 10$, find all prime numbers $p \leq 20$ for which $p + 1$ are B-powersmooth numbers.

(a) As in 2.2 we are looking for prime numbers $p \leq 20$ for which $p+1 \mid 12$, which are

$$3-1=2,\ 4-1=3,\ 6-1=5,\ 12-1=11.$$

(b) Again, we add the prime numbers

$$8-1=7,\ 18-1=17,\ 20-1=19.$$

□

3 ECM algorithm

Let $a, b \in \mathbb{Z}_N$ such that $\gcd(4a^3+27b^2, N)=1$. Recall the definition of the unary operation $\ominus$ and partial commuutative binary operation $\oplus$ on $\mathbb{Z}_N^2 \cup \{o\}$. Denote $\gamma=(\gamma_1,\gamma_2), \delta=(\delta_1,\delta_2)\eta=(\eta_1,\eta_2) \in \mathbb{Z}_N^2$. Then

(1) $\ominus\gamma=(\gamma_1,-\gamma_2)$, $\ominus o=o$

(2) $\gamma \oplus o=\gamma$, $(\ominus\gamma)\oplus\gamma=o$

(3) let $\gamma \neq \ominus\delta$ and $\eta:=\gamma\oplus\delta$, then
$\eta=(\lambda^2-\gamma_1-\delta_1, \lambda(\gamma_1-\eta_1)-\gamma_2)$ if there exists λ satisfying
(a) $\lambda=\frac{\delta_2-\gamma_2}{\delta_1-\gamma_1}$ provided $\gamma_1 \neq \delta_1$ and $\gcd(\delta_1-\gamma_1, N)=1$,
(b) $\lambda=\frac{3\gamma_1^2+a}{\gamma_2+\delta_2}$ provided $\gamma_1=\delta_1$ and $\gcd(\gamma_2+\delta_2, N)=1$

We denote by (R1) the rule for addition given by items (1) a (2), by (R2) the rule for addition (3a) and by (R3) the rule given by (3b).

Recall the Algorithm 7

`INPUT:` N $a, b \in \mathbb{Z}_N$, $A, B \in \mathbb{Z}_N^2 \cup \{o\}$: $\gcd(6(4a^3+27b^2), N)=1$
`OUTPUT: a proper divisor of` N `or` $A \oplus B$

`0. if` $A=o$ `then return` B `else if` $B=o$ `then return` A,

`1.` $(\alpha_1,\alpha_2):=A$, $(\beta_1,\beta_2):=B$,

`2. if` $\alpha_1 \neq \beta_1$ `then if` $d:=\gcd(\alpha_1-\beta_1, N)>1$ `then return` d
`else return` $A \oplus B$

`3. if` $\alpha_2 \equiv -\beta_2 \pmod N$ `then return` o,

`4. if` $d:=\gcd(\alpha_2+\beta_2, N)>1$ `then return` d
`else return` $A \oplus B$

Define for $p \mid N$ the mapping $\pi_p : \mathbb{Z}_N^2 \cup \{o\} \to \mathbb{Z}_p^2 \cup \{o\}$ by the rule $\pi_p(\alpha_1, \alpha_2) = ((\alpha_1) \bmod p, (\alpha_2) \bmod p)$ and $\pi_p(o) = o$.

3.1. Let $A, B \in \mathbb{Z}_N^2 \cup \{o\}$ such that $\pi_p(A), \pi_p(B) \in E_{a,b}(\mathbb{Z}_p)$ for prime $p \mid N$. Prove that if ALG_7 does not return a proper divisor, then it outputs $A \oplus B$ and $\pi_p(A \oplus B) = \pi_p(A) \oplus \pi_p(B) \in E_{a,b}(\mathbb{Z}_p)$.

We discuss all possible outputs of the algorithm:

step 2. If $d := \gcd(\alpha_1 - \beta_1, N) > 1$, then $d < N$ since $|\alpha_1 - \beta_1| < N$, hence d is a proper divisor of N.
If $d = 1$, then $\alpha_1 \not\equiv \beta_1 \pmod p$, hence $A \oplus B$ and $\pi_p(A) \oplus \pi_p(B)$ is calculated by (R2), hence $\pi_p(A \oplus B) = \pi_p(A) \oplus \pi_p(B) \in E_{a,b}(\mathbb{Z}_p)$.

step 3. If $\alpha_1 = \beta_1$ and $\alpha_2 \equiv -\beta_2 \pmod N$, then $\alpha_2 \equiv -\beta_2 \pmod p$, and so $A \oplus B$ and $\pi_p(A) \oplus \pi_p(B)$ is calculated by (R1), which means that $\pi_p(A \oplus B) = \pi_p(o) = \pi_p(A) \oplus \pi_p(B) \in E_{a,b}(\mathbb{Z}_p)$.

step 4. We have $\alpha_1 - \beta_1$ and $\alpha_2 + \beta_2 \equiv 0 \pmod N$.
If $d := \gcd(\alpha_2 + \beta_2, N) > 1$, then $d < N$ since $\alpha_2 + \beta_2$ is not divisible by N.
If $d = 1$, then $\alpha_2 + \beta_2 \not\equiv 0 \pmod p$ and both additions $A \oplus B$ and $\pi_p(A) \oplus \pi_p(B)$ are calculated by (R3), thus $\pi_p(A \oplus B) = \pi_p(A) \oplus \pi_p(B) \in E_{a,b}(\mathbb{Z}_p)$ again.

Note that we have shown more then it is stated in 3.1, we have proved that outputs $A \oplus B$ and $\pi_p(A) \oplus \pi_p(B)$ are calculated by the same rule (R1)/(R2)/(R3) if have found no collision. □

3.2. Compute all elements of the groups (a) $E_{1,1}(\mathbb{Z}_7)$ and (b) $E_{1,1}(\mathbb{Z}_{11})$ and decide whether the groups are cyclic.

(a) Recall that $E_{1,1}(\mathbb{Z}_7) = \{(x, y) \in \mathbb{Z}_7 \mid y^2 \equiv x^3 + x + 1 \pmod 7\} \cup \{o\}$ and observe that $y^2 \in Y = \{0, 1, 4, 2\}$. Now, we calculate, which values of x satisfies $x^3 + x + 1 \in Y$:

	0	1	2	3	4	5	6
$x^3 + x$	0	2	3	2	5	4	5
$x^3 + x + 1$	1	3	4	3	6	5	6

Thus we can easily find all elements

$$E_{1,1}(\mathbb{Z}_7) = \{(0, 1), (0, 6), (2, 2), (2, 5), o\}$$

Since the order $|E_{1,1}(\mathbb{Z}_7)| = 5$ is prime, $E_{1,1}(\mathbb{Z}_7) \cong \mathbb{Z}_5$.

(b) We proceed by the same way as in (a), first let us observe that $y^2 \in Y = \{0, 1, 4, 9, 5, 3\}$ and calculate $x^3 + x + 1 \in Y$:

	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x$	0	2	-1	-3	2	4	-4	-2	3	1	-2
$x^3 + x + 1$	1	3	0	-2	3	5	-3	-1	4	2	-1

Thus

$$E_{1,1}(\mathbb{Z}_{11}) = \{(0, \pm 1), (1, \pm 5), (2, 0), (3, \pm 3), (4, \pm 5), (5, \pm 4), (8, \pm 2), o\}.$$

Since $E_{1,1}(\mathbb{Z}_{11})$ is an abelian group of order 14, it is a cyclic group, hence $E_{1,1}(\mathbb{Z}_{11}) \cong \mathbb{Z}_{14}$. □

3.3. Let $P = (0, 1)$.

(a) determine the order of the element P in the groups $E_{1,1}(\mathbb{Z}_7)$ and $E_{1,1}(\mathbb{Z}_{11})$,

(b) calculate the cardinality $|E_{1,1}(\mathbb{Z}_{77})|$,

(c) either calculate the values or find a collision when calculating $Q = P \oplus P$, $R = Q \oplus Q$, $S = R \oplus P$ in $\mathbb{Z}_N^2 \cup \{o\}$,

(d) determine the result of the calculation from (c) in the groups $E_{1,1}(\mathbb{Z}_7)$ and $E_{1,1}(\mathbb{Z}_{11})$.

(a) Since $P \neq o$ and the group $E_{1,1}(\mathbb{Z}_7)$ is of the prime order 5, the element P must be a generator, i.e., it is of order 5.

In the cyclic group $E_{1,1}(\mathbb{Z}_{11})$ of order 14, there are elements of order 1, 2, 7, and 14, so it suffices to calculate $[2]P$ and $[7]P$ to determine the order of P. If we denote $(\gamma_1, \gamma_2) = [2]P$, then

$$\gamma_1 = \lambda^2 - 2 \cdot 0 = 5^2 - 2 \cdot 0 = 3, \text{ because } \lambda = \frac{3 \cdot 0^2 + 1}{2 \cdot 1} = -5,$$

$$\gamma_2 = \lambda(0 - \gamma_1) - 1 = -5(0 - 3) - 1 = 3, \text{ therefore } [2]P = (3, 3).$$

Furthermore, for $(\gamma_1, \gamma_2) = [4]P = [2](3, 3)$, we obtain $\lambda = \frac{3 \cdot 3^2 + 1}{2 \cdot 3} = 1$,

$$\gamma_1 = \lambda^2 - 2 \cdot 3 = 1^2 - 6 = -5, \ \gamma_2 = \lambda(3 - \gamma_1) - 3 = 1(3 + 5) - 3 = 5,$$

therefore $[4]P = (-5, 5)$.

Now we calculate $(\gamma_1, \gamma_2) = [3]P = P \oplus [2]P = (0, 1) \oplus (3, 3)$:

$$\gamma_1 = \lambda^2 - 0 - 3 = 3^2 - 3 = -5, \text{ because } \lambda = \frac{1 - 3}{0 - 3} = -3,$$

$$\gamma_2 = \lambda(0 - \gamma_1) + 5 = -3(0 + 5) - 1 = -5, \text{ and therefore } [3]P = (-5, -5).$$

Now we can see that $[4]P = \ominus[3]P$, which means that $[7]P = o$, and since we have already found that $P \neq o$ and $P \neq \ominus P$, the element P in the group $E_{1,1}(\mathbb{Z}_{11})$ has order 7.

30.03.

(b) We realize that the mapping

$$\Psi : \{(x, y) \in \mathbb{Z}_{77}^2 \mid y^2 \equiv x^3 + x + 1 \pmod{77}\} \rightarrow$$

$$\{(x, y) \in \mathbb{Z}_7^2 \mid y^2 \equiv x^3+x+1 \pmod 7\} \times \{(x, y) \in \mathbb{Z}_{11}^2 \mid y^2 \equiv x^3+x+1 \pmod{11}\}$$

given by the rule $\Psi(x, y) = ((x) \bmod 7, (y) \bmod 7), (x) \bmod 11, (y) \bmod 11))$ gives a bijection thanks to the Chinese remainder theorem. Since the mapped set is precisely $E_{1,1}(\mathbb{Z}_{77}) \setminus \{o\}$ and its image is the Cartesian product of the sets $E_{1,1}(\mathbb{Z}_{77}) \setminus \{o\}$ and $E_{1,1}(\mathbb{Z}_{11}) \setminus \{o\}$ we obtain

$$|E_{1,1}(\mathbb{Z}_{77})| = |(E_{1,1}(\mathbb{Z}_{77}) \setminus \{o\}) \times (E_{1,1}(\mathbb{Z}_{11}) \setminus \{o\})| + 1 = 4 \cdot 13 + 1 = 53.$$

(c) We will proceed as in task (a). To determine $(\gamma_1, \gamma_2) = [2]P$ on $E_{1,1}(\mathbb{Z}_{77})$, we need to calculate $\lambda = \frac{3 \cdot 0^2 + 1}{2 \cdot 1} = 2^{-1} = -38$ and then

$$\gamma_1 = \lambda^2 - 2 \cdot 0 = 38^2 - 2 \cdot 0 = -19, \ \gamma_2 = \lambda(0 - \gamma_1) - 1 = -38(0 + 19) - 1 = -30.$$

So we have found $Q = (-19, -30)$. Again, we duplicate $(\gamma_1, \gamma_2) = R = [2]Q$, so we calculate the slope of the corresponding tangent line $\lambda = \frac{3 \cdot 19^2 + 1}{2 \cdot (-30)} = \frac{6}{-60} = \frac{-8}{80} = \frac{69}{3} = 23$ and then

$$\gamma_1 = 23^2 - 2 \cdot (-19) = 28, \ \gamma_2 = 23(-19 - 28) + 30 = 27,$$

so $R = (28, 27)$ and finally, if we are looking for $P \oplus R$, then when attempting to calculate the intersection λ, we see that $\gcd(28, 77) = 7$, so we have a found collision and the proper divisor 7 of the number 77.

(d) Since in $E_{1,1}(\mathbb{Z}_7)$ and in $E_{1,1}(\mathbb{Z}_{11})$ when calculating $Q = P \oplus P$, $S = Q \oplus Q$, $R = S \oplus P$, we use the same formula with a different modulus that divides the original modulus 77, and we only need to adjust the result with the appropriate modulus. Thus, we obtain in $E_{1,1}(\mathbb{Z}_7)$:

$$Q = ((-19)) \bmod 7, (-30) \bmod 7) = (2, -2)$$

$$R = ((28)) \bmod 7, (27) \bmod 7) = (0, -1)$$

and we immediately see that $R = \ominus P$, therefore $S = R \oplus P = [5]P = o$, which is consistent with the finding about the order of the element P from task (a).

We have already determined the values of Q and R in $E_{1,1}(\mathbb{Z}_{11})$ in calculation (a), so let us repeat that we have

$$Q = ((-19)) \bmod 11, (-30) \bmod 11) = (3, 3)$$

$$R = ((28)) \bmod 11, (27) \bmod 11) = (-5, 5)$$

and we are left with either the standard procedure of calculating $(\gamma_1, \gamma_2) = S = R \oplus P = [5]P$, where the slope of the tangent line is $\lambda = \frac{5-1}{-5-0} = \frac{2}{3} = -3$ and

$$\gamma_1 = 3^2 + 5 - 0 = 3, \quad \gamma_2 = -3(0 - 3) - 1 = -3,$$

or we realize that from the knowledge of the order of the element P and the value $[2]P = (3, 3)$, which we found in (a), it follows that $[5]P = \ominus[2]P = \ominus(3, 3) = (3, -3)$. □

3.4. If you know that $|E_{1,1}(\mathbb{Z}_{199})| = 218$, $|E_{1,1}(\mathbb{Z}_{269})| = 294$, and $53531 = 199 \cdot 269$, explain why for e_{49} and $P = (0, 1) \in E_{1,1}(\mathbb{Z}_{53531})$ we can expect ECM to find a non-trivial divisor of the number 53531.

We can easily calculate the prime factorizations $218 = 2 \cdot 109$ and $294 = 2 \cdot \cdot 3 \cdot 7^2$, from which it follows that $\gcd(218, 294) = 2$. Since $P \neq \ominus P$ in both groups $E_{1,1}(\mathbb{Z}_{199})$ and $E_{1,1}(\mathbb{Z}_{269})$, and if the element P in $E_{1,1}(\mathbb{Z}_{199})$, it must be of order 109 or 218, while if $[k]P = 0$ in $E_{1,1}(\mathbb{Z}_{269})$, then $2 < k \mid 294$. If during the calculation we do not encounter $k \leq e = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \mid e_{49}$, which would be the exponent of P in $E_{1,1}(\mathbb{Z}_{199})$, then we know for sure that $[e]P = 0$ in $E_{1,1}(\mathbb{Z}_{269})$, and therefore we will obtain a collision when calculating $[e]P$ in $E_{1,1}(\mathbb{Z}_{53531})$. The only situation that is undesirable from the point of view of our test is where k would be the exponent of P in both groups considered; it would certainly be a multiple of the prime number 109 and the divisor $3 \cdot 7^2$, so if we avoid multiples of 109 in the calculation, we can expect to find a proper divisor. □

20.04.

4 Roots modulo N

4.1. Let $p \in \mathbb{P}$ be an odd number such that $p \equiv 3 \pmod 4$ and $a \in \mathbb{Z}_p^*$. If there exists a solution to the equation $x^2 = a$ for $a \in \mathbb{Z}_p^*$, verify that it is of the form $x = \pm a^{\frac{p+1}{4}}$.

Note that $4 \mid p+1$ and that a solution of the equation $x^2 = a$ exists if and only if $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = 1$. Therefore

$$(a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} = a,$$

so $x = \pm a^{\frac{p+1}{4}}$. □

4.2. Let $p = 8k+5 \in \mathbb{P}$ for $k \in \mathbb{N}$ (i.e., $p \equiv 5 \pmod 8$) and $a \in \mathbb{Z}_p^*$. Prove that if there is a solution of the equation $x^2 = a \in \mathbb{Z}_p^*$, it is precisely of the form $x = \pm a^{k+1}$ or $x = \pm 2^{2k+1} a^{k+1}$.

Let a be a quadratic residue modulo p. Since $\frac{p-1}{2} = 4k+2$, we have $a^{4k+2} = 1$, so a^{2k+1} is of the exponent 2, and therefore $a^{2k+1} = \pm 1$.

If $a^{2k+1} = 1$, then $a^{2k+2} = a$, and therefore the solution to our equation is $x = \pm a^{k+1}$.

If $a^{2k+1} = -1$, we recall that $2^{4k+2} = \left(\frac{2}{p}\right) = -1$, since 2 is a quadratic residue modulo the prime number p precisely when $p \equiv \pm 1 \pmod 8$, which means that $2^{4k+2} a^{2k+1} = 1$, so $2^{4k+2} a^{2k+2} = a$ and $x = \pm 2^{2k+1} a^{k+1}$ is the solution. □

4.3. Find all solutions to the equation $x^2 = a$ for $a \in \mathbb{Z}_p^*$ for

(a) $p = 31$, $a = 20$,

(b) $p = 31$, $a = 11$,

(c) $p = 101$, $a = 24$,

(d) $p = 101$, $a = 70$.

Since $31 \equiv 3 \pmod 4$, it suffices in examples (a) and (b) to use the result of Exercise 4.1, calculate $x = \pm a^{k+1}$, and verify that $x^2 = a$ (or check beforehand whether a is a quadratic residue):

(a) $x = 20^{\frac{32}{4}} = (-11)^8 = (-3)^4 = 12$ and $x^2 = 20$, so $x = \pm 12$.

(b) $x = 11^{\frac{32}{4}} = (-3)^4 = 12$ and $x^2 \neq 11$, so the equation has no solution.

In problems (c) and (d), we will use the result 4.2 analogously to (a) and (b), since $101 \equiv 5 \pmod 8$ and $101 = 8k+5$ for $k = 12$. First, in $\mathbb{Z}_{101}$, we compute $2^{2k+1} = 2^{25} = 10$, then we compute $y = a^{k+1}$. If $y^2 = a$, we will have the solution $\pm y$. Otherwise, we check whether $-y^2 = a$, i.e., whether $(2^{25} y)^2 = (10y) = a$, and if so, the solution to the problem will be $\pm 10y$; otherwise, the problem has no solution.

(c) We calculate $y = 24^{k+1} = 24^{13} = -23$, and since $y^2 = 24$, we have the solution $x = \pm 23$.

(d) Now $y = 70^{13} = 43$, and since $y^2 = 31 = -70$, we see that a solution exists and must be of the form $x = \pm 10 \cdot 43 = \pm 26$. □

4.4. Find all the roots of the polynomial $3x^2 + 7x - 27$ in the field $\mathbb{Z}_{101}$.

First, we calculate the determinant of the polynomial $7^2 + 4 \cdot 3 \cdot 27 = 70$. In Exercise 4.3(d), we have already found that $\sqrt{70} = \pm 26$; now we need only apply the standard formula

$$x = -\frac{7}{6} \pm \frac{26}{6} = -7 \cdot 17 \pm 26 \cdot 17 = -18 \pm 38.$$

We have found that the polynomial $3x^2 + 7x - 27$ has roots 20 and 45 in $\mathbb{Z}_{101}$. □

4.5. Using the Tonelli-Shanks algorithm, find all solutions to the equation $x^2 = 5$ in the field $\mathbb{Z}_{41}$.

Since $41 - 1 = 2^3 \cdot 5$, we have $e = 3$ and $m = 5$.

First, we need to find an element of order 2^3. If we choose $z_0 = 2$ and $z = z_0^m = 2^5 = -9$, then $9^2 = -1$, so $o_{\mathbb{Z}_{41}^*}(9) = 4$. If we choose $z_0 = 3$, then $3^5 = -3$, and since $3^4 = 9^2 = -1$, we see that $o_{\mathbb{Z}_{41}^*}(3) = 8$, so we can choose $z = 3$ (instead of -3, which we would have obtained in the Tonelli-Shanks algorithm for $z_0 = 3$).

Now we can initialize the algorithm:

$$y := z = 3, \quad r := e = 3, \quad b := 5^m = 5^5 = 9, \quad x := 5^{\frac{m+1}{2}} = 5^3 = 2$$

and compute the order $o_{\mathbb{Z}_{41}^*}(b) = o_{\mathbb{Z}_{41}^*}(9) = 2^2$, so $s = 2$. Since $s \neq 0, 3$, we proceed to calculate

$$t := y^{2^{r-s-1}} = 3, \quad y := t^2 = 9, \quad r := s = 2, \quad x := xt = 6, \quad b := by = 9^2 = -1$$

and then return to calculating the order of the new element b: $o_{\mathbb{Z}_{41}^*}(-1) = 2^1$ and obtain a new $s = 1$.

Once again, the algorithm does not terminate in this test case because $s \neq 0, 2$, so we continue calculating

$$t := 9^{2^{2-1-1}} = 9, \quad y := t^2 = -1, \quad r := s = 1, \quad x := x \cdot t = 13, \quad b := (-1)^2 = 1$$

We see that the element b has order one, so the algorithm returns the value 13 in the test, and ± 13 are precisely the square roots of 5 in $\mathbb{Z}_{41}$. □

4.6. In the field $\mathbb{Z}_{17}$, find all the roots of the polynomials

(a) $x^2 + x + 13$,

(b) $x^2 - 2x - 1$.

(a) First, we calculate the discriminant $D = 1^2 - 4 \cdot 13 = 0$ and then easily determine the single double root $-\frac{1}{2} = 8$, i.e., $x^2 + x + 13 = (x - 8)^2$.

(b) Again, we determine the discriminant $D = (-2)^2 + 4 \cdot 1 = 8$, which we need to square root in the field $\mathbb{Z}_{17}$. We can again use the Tonelli-Shanks algorithm, where $17 - 1 = 2^4$, and easily find that, for example, the element $z = 3$ generates $\mathbb{Z}_{17}^*$, so it is an element of order 16. Therefore, we obtain

$$y := 3, \quad r := 4, \quad b := 8, \quad x := 8, \quad s := 3$$

because $o_{\mathbb{Z}_{17}^*}(8) = 2^3$. Since the algorithm does not terminate, we compute the values

$$t := y^{2^0} = 3, \;\; y := t^2 = -8, \;\; r := s = 3, \;\; x := xt = 7, \;\; b := by = 8 \cdot (-8) = 4$$

and determine the order $o_{\mathbb{Z}_{17}^*}(b) = o_{\mathbb{Z}_{17}^*}(4) = 2^2$, so $s = 2$. Since $s \neq 0, 3$, we calculate again

$$t := (-8)^{2^0} = -8, \;\; y := t^2 = -4, \;\; r := s = 2, \;\; x := xt = 5, \;\; b := by = 4 \cdot (-4) = 1.$$

Since $b = 1$, we have obtained the desired square root of the determinant $x = 5$, and it remains to apply the standard formula

$$x = \frac{2}{2} \pm \frac{5}{2} = 1 \pm 11,$$

we found the roots -5 and 8, so $x^2 - 2x - 1 = (x + 5)(x - 7)$. □

4.7. Find some solutions to the congruence $x^2 \equiv 44 \pmod{n}$, given that

(a) $n = 125$,

(b) $n = 81$,

(c) $n = 375$,

(d) $n = 49$,

(e) $n = 125 \cdot 49 = 6125$,

(a) First, we easily find the solution $x = 2$ to the congruence

$$x^2 \equiv 44 \equiv 4 \pmod{5},$$

which we then lift using Hensel's algorithm. Now we determine $t = -1$ satisfying $2xt \equiv -t \equiv 1 \pmod{5}$. Then, in the for-loop, we first find $y = \frac{2^2-44}{5} = 2$ in $\mathbb{Z}_5$, $z = -ty = 2$, and compute the new $x = (2 + 2 \cdot 5) \bmod 25 = 12$. In the second iteration of the for-loop, we set $y = (\frac{12^2-44}{25}) \bmod 5 = 4$, then $z = -ty = 4$, and therefore $x = (12 + 4 \cdot 25) \bmod 125 = -13$, which is the solution we are looking for.

(b) Since $(44) \bmod 3 = 2$ is not a quadratic residue, the equation has no solution of modulus 3^k for any $k \leq 1$.

(c) Thanks to the Chinese Remainder Theorem applied to $375 = 3 \cdot 125$, any solution would also be a solution to the congruence $x^2 \equiv 44 \pmod{3}$, which we realized in (b) does not exist. Thus, we have no solution in this case either.

(d) We proceed as in (a). We easily find the solution $x = 3$ to the congruence $x^2 \equiv 44 \equiv 2 \pmod{7}$, and then we need only perform a single step of Hensel's lifting: we compute $t = -1$ such that $2 \cdot 3t \equiv -t \equiv 1 \pmod{7}$, find $y = \frac{3^2-44}{5} = 2$ in $\mathbb{Z}_7$, $z = -ty = 2$, and determine $x = (3+2\cdot 7) \bmod 49 = 17$.

(e) This time, we obtain the solution by standardly applying the Chinese Remainder Theorem to the solutions found in (a) and (d); that is, we seek $x \in \mathbb{Z}_{6125}$ satisfying the congruences

$$x \equiv -13 \pmod{125}, \quad x \equiv 17 \pmod{49},$$

which we can solve, for example, using Garner's algorithm. For $x = -13 + 125a$ we have

$$-13 + 125a \equiv 17 \pmod{49} \;\Rightarrow\; 27a \equiv 30 \pmod{49} \;\Rightarrow$$

$$\Rightarrow\; 5a \equiv 60 \pmod{49} \;\Rightarrow\; a \equiv 12 \pmod{49}.$$

Thus, we have found the solution $x = -13 + 125 \cdot 12 = 1487$. □

5 Dixon's factorization and CFRAC

5.1. Find continued fractions:

(a) $\sqrt{17}$,

(b) $\sqrt{23}$,

(c) $3+\sqrt{23}$,

(a) Using Algorithm 16 from the lecture, we calculate the initial values $a_0 = g = \lfloor\sqrt{17}\rfloor = 4$, $R_0 = 0$, $S_0 = 1$, and then we are going on recursively

$$R_{n+1} = a_n S_n - R_n, \quad S_{n+1} = \frac{N - R_{n+1}^2}{S_n}, \quad a_{n+1} = \lfloor\frac{R_{n+1}+g}{S_{n+1}}\rfloor.$$

Then we will write the values into a table

i	0	1	2
R_i	0	4	4
S_i	1	1	1
a_i	4	8	8

In step $i = 2$, we obtaine the same values $R_2 = R_1$ and $S_2 = S_1$ as in step $i = 1$, so we have a period of length 1, and the resulting continued fraction is of the form $\sqrt{17} = [4, \overline{8}]$.

(b) We proceed as in (a), i.e., for the initial values $a_0 = \lfloor\sqrt{23}\rfloor = 4$, $R_0 = 0$, $S_0 = 1$, we calculate the values by recursion

$$R_{n+1} = a_n S_n - R_n, \quad S_{n+1} = \frac{23 - R_{n+1}^2}{S_n}, \quad a_{n+1} = \lfloor\frac{R_{n+1}+4}{S_{n+1}}\rfloor$$

until we find the first pair $i < j$ for which $(R_i, S_i) = (R_j, S_j)$:

i	0	1	2	3	4	5
R_i	0	4	3	3	4	4
S_i	1	7	2	7	1	7
a_i	4	1	3	1	8	1

We can see that $(R_1, S_1) = (R_5, S_5) = (4, 7)$, so we have a period of length 4 and a continued fraction $\sqrt{23} = [4, \overline{1, 3, 1, 8}]$.

(c) Now we simply need to shift the value from (b) appropriately, that is

$$3 + \sqrt{23} = 3 + [4, \overline{1, 3, 1, 8}] = [7, \overline{1, 3, 1, 8}].$$

□

5.2. Find the number α with the given eventually periodic series expansion, if

(a) $\alpha = [\overline{6}]$,

(b) $\alpha = [\overline{1,4}]$,

(c) $\alpha = [\overline{3,2,1}]$,

(d) $\alpha = [2,3,\overline{6}]$.

For periodic continued fractions $\alpha = [\overline{a_0,\ldots,a_k}]$, recall that

$$[\overline{a_0,\ldots,a_k}] = [a_0,\ldots,a_k,[\overline{a_0,\ldots,a_k}]]$$

from which follows the relation $\alpha = \frac{p_k\alpha+p_{k-1}}{q_k\alpha+q_{k-1}}$.

(a) The relation $\alpha = \frac{6\alpha+1}{1\alpha} = 6+\frac{1}{\alpha}$ mentioned here can be obtained directly from the definition. We are therefore looking for a positive α satisfying $\alpha^2 = 6\alpha+1$, i.e., a positive root of the polynomial x^2-6x-1, which is clearly the value $\alpha = 3+\sqrt{10}$.

(b) We know that $(p_{-1},q_{-1}) = (1,0)$ and $(p_0,q_0) = (1,1)$, so we can easily calculate

$$(p_1,q_1) = 4(p_0,q_0)+(p_{-1},q_{-1}) = (4,4)+(1,0) = (5,4),$$

so $\alpha = \frac{p_1\alpha+p_0}{q_1\alpha+q_0} = \frac{5\alpha+1}{4\alpha+1}$ and we again seek a positive root of the polynomial $4x^2-4x-1$, which is the value $\alpha = \frac{1}{2}+\frac{\sqrt{2}}{2}$.

(c) Again, we have $(p_{-1},q_{-1}) = (1,0)$ and $(p_0,q_0) = (3,1)$, and we find as usual

$$(p_1,q_1) = 2(3,1)+(1,0) = (7,2), \quad (p_2,q_2) = 1(7,2)+(3,1) = (10,3),$$

which leads to finding α satisfying $\alpha = \frac{10\alpha+7}{3\alpha+2}$, which is a root of the polynomial $3x^2-8x-7$, namely $\alpha = \frac{4}{3}+\frac{\sqrt{47}}{3}$ □

(d) Using the values from part (a) and the definition that states that

$$[2,3,\overline{6}] = [2[3[\overline{6}]]] = 2+\frac{1}{3+\frac{1}{3+\sqrt{10}}} = 2+\frac{1}{\sqrt{10}},$$

we see that $\alpha = 2+\frac{\sqrt{10}}{10}$. □

In notation of Lemma 5.2 we say that e_I is a *bad solution* of the linear homogeneous equations $xA = 0$, if for the corresponding pair (x,y) either $N \mid x-y$ or $N \mid x+y$.

5.3. Let (x_i, y_i) be, for $i = 1, \ldots, k$, smooth relations with respect to the basis B for a natural number N, such that $\gcd(y_i, N) = 1$. Prove that the set of bad solutions $e_I \in \mathbb{F}_2^k$ forms a subspace of the vector space $\mathbb{F}_2^k$.

First, recall that a pair (x_i, y_i) is a smooth relation if

$$x_i^2 \equiv y_i \pmod{N} \quad \text{and} \quad y_i = \prod_{b \in B} b^{v_b(y_i)}$$

and $e_I \in \mathbb{F}_2^k$ is a solution if and only if $\sum_{i \in I} v_b(y_i)$ is even for every $b \in B$, that is

$$\prod_{i \in I} x_i^2 \equiv \prod_{i \in I} y_i \equiv y^2 \pmod{N} \quad \text{for} \quad y = \prod_{b \in B} b^{\frac{1}{2} \sum_{i \in I} v_b(y_i)}.$$

The solution is bad if, in addition,

$$\prod_{i \in I} x_i \equiv \pm y \equiv \pm \prod_{b \in B} b^{\frac{1}{2} \sum_{i \in I} v_b(y_i)} \pmod{N}.$$

Since we consider a solution to be a subspace of the vector space F_2^k over the field F_2, it suffices to prove that the sum of two bad solutions $e_I + e_J = e_{I \div J}$ is again a bad solution, where $I \div J = I \cup J \setminus (I \cap J)$. First, we note that

$$\prod_{i \in I} x_i \prod_{j \in J} x_j \equiv \pm \prod_{b \in B} b^{\frac{1}{2}(\sum_{i \in I} v_b(y_i) + \sum_{j \in J} v_b(y_j))} \pmod{N}.$$

11.05.

We rearrange both sides of the congruence to

$$\text{(K)} \quad \prod_{i \in I \div J} x_i \cdot \prod_{j \in I \cap J} x_j^2 \equiv \pm \prod_{b \in B} b^{\frac{1}{2}(\sum_{i \in I \div J} v_b(y_i))} \cdot \prod_{b \in B} b^{(\sum_{i \in I \cap J} v_b(y_i))} \pmod{N}.$$

where we note that

$$\frac{1}{2}\Big(\sum_{i \in I \div J} v_b(y_i)\Big) = \frac{1}{2}\Big(\sum_{i \in I} v_b(y_i) + \sum_{j \in J} v_b(y_j)\Big) - \sum_{i \in I \cap J} v_b(y_i)\Big)$$

is a non-negative integer, so the power on the right is correctly defined. Furthermore, from the definition of a smooth relation, we have the congruence

$$\prod_{i \in I \cap J} x_i^2 \equiv \prod_{i \in I \cap J} y_i \equiv \prod_{i \in I \cap J} \prod_{b \in B} b^{v_b(y_i)} \equiv \prod_{b \in B} b^{(\sum_{i \in I \cap J} v_b(y_i))} \pmod{N}.$$

Since, by assumption, $\prod_{i\in I\cap J} y_i$ is coprime to N, there exists u such that

$$1 \equiv u \cdot \prod_{i\in I\cap J} y_i \equiv u \cdot \prod_{i\in I\cap J} x_i^2 \equiv u \cdot \prod_{b\in B} b^{(\sum_{i\in I\cap J} v_b(y_i))} \pmod{N}$$

and therefore, by multiplying both sides of the congruence (K) by u, we obtain the congruence

$$\prod_{i\in I\div J} x_i \equiv \pm \prod_{b\in B} b^{\frac{1}{2}(\sum_{i\in I\div J} v_b(y_i))} \pmod{N},$$

so $e_{I\div J}$ is again a bad solution. □

18.05.

5.4. Prove that for $\sqrt{N} \notin \mathbb{Q}$, the values R'_n, S_n, a_n, r_n from Algorithm 17 (CFRAC) are non-negative and less than $2\sqrt{N}$ for all $n > 0$.

Let us consider an arbitrary $n > 0$. By definition, we know that $r_n \geq 0$ and $a_n > 0$, and in Theorem 5.7 we showed that $S_n > 0$, so $R'_n = a_n S_n + r_n > 0$. Furthermore, from the recurrence relation $R_n = R'_n - g$, where $g = \lfloor\sqrt{N}\rfloor$, it follows that $N^2 - R_n = S_n S_{n-1} > 0$, which means that $|R_n| < \sqrt{N}$, and thus $R'_n < g + \sqrt{N} < 2\sqrt{N}$. Finally, for $a_n S_n + r_n = R'_n \leq 2g$, we have that for $n > 0$ all values are non-negative integers and a_n, S_n are positive, and therefore $a_n, S_n, r_n \leq 2g < 2\sqrt{N}$. □