MA7010 – Number Theory for Cryptography - Assignment 3

Ajeesh Thattukunnel Vijayan

January 11^{th} 2024

1 Introduction

Name	a	b	c	d	Q6
Ajeesh	2929	20953	500657	23861	ii

Table 1: Input Numbers For Ajeesh

2 Answers

1. For the number a given to you on page 1 answer the following:

   a. Show that a can be written as the sum of squares in two different ways

   Answer:

   $a = 2929$
   Let $u = 5, v = 2, w = 10, x = 1$
   Brahmagupta Identity helps us to write this numbers in two different sum of squares form
   $(u^2 + v^2)(w^2 + x^2) = (uw - vx)^2 + (ux + vw)^2$
   $= (uw + vx)^2 + (ux - vw)^2$
   $\therefore (uw - vx)^2 + (ux + vw)^2 = (5 \times 10 - 2 \times 1)^2 + (5 \times 1 + 2 \times 10)^2 = 48^2 + 25^2$
   and $(uw + vx)^2 + (ux - vw)^2 = (5 \times 10 + 2 \times 1)^2 + (5 \times 1 - 2 \times 10)^2 = 52^2 + (-15)^2$
   Hence the two different sum of squares forms of 2929 are:
   $2929 = 48^2 + 25^2$
   $2929 = 52^2 + 15^2$ $\blacksquare$

   b. Hence apply Euler's method to factorise a.

   Answer:

   From 1.(a) above, we have
   $2929 = 48^2 + 25^2 = a^2 + b^2$
   $2929 = 52^2 + 15^2 = c^2 + d^2$
   $\therefore a^2 + b^2 = c^2 + d^2$
   $\implies a^2 - c^2 = b^2 - d^2$
   $\implies (a - c)(a + c) = (b - d)(b + d)$

Let $k = gcd(a-c, b+d)$ and $h = gcd(a+c, b+d)$

$\therefore k = 2$ and $h = 20$

$\implies a - c = k.l \implies 4 = 2 \times l \implies l = 2$

$b - d = k.m \implies 10 = 2 \times m \implies m = 5$

$a + c = h.m' \implies 100 = 20 \times m' \implies m' = 5$

$b + d = h.l' \implies 40 = 20 \times l' \implies l' = 2$

$\therefore n = 2929 = ((\frac{k}{2})^2 + (\frac{h}{2})^2)(l^2 + m^2)$

$= (1^2 + 10^2)(2^2 + 5^2) = (101 \times 29)$ ■

2. (a) Take the number b assigned to you on page 1 and apply the gcd method to find its smallest factor.

Answer:

$b = 20953$

Set $k = \lfloor \sqrt{b} \rfloor = 144$

$$P_0 = \prod_{primes<144} p = 1001464665059919006750923313164994005736633465320043309 0$$

$gcd(10014646650599190067509233131649940057366334653200433090, 20953) = 23$,

which is the smallest factor of 20953 ■

The Maple worksheet for this exercise is below:

> $p0 := 1$

$$p0 := 1 \tag{1}$$

> $k := 2;$

$$k := 2 \tag{2}$$

> while $k < 144$ do $p0 := p0 \cdot k;$
$k := nextprime(k);$
od;

$p0 := 2$

$k := 3$

$p0 := 6$

$k := 5$

$p0 := 30$

$k := 7$

$p0 := 210$

$k := 11$

$p0 := 2310$

$k := 13$

$p0 := 30030$

$k := 17$

$p0 := 510510$

$k := 19$

$p0 := 9699690$

$k := 23$

$p0 := 223092870$

$k := 29$

$p0 := 6469693230$

$k := 31$

$p0 := 200560490130$

$k := 37$

$p0 := 7420738134810$

$k := 41$

$p0 := 304250263527210$

$k := 43$

$p0 := 13082761331670030$

$k := 47$

$p0 := 614889782588491410$

$k := 53$

$p0 := 32589158477190044730$

$k := 59$

$p0 := 1922760350154212639070$

$k := 61$

$p0 := 117288381359406970983270$

$k := 67$

$p0 := 7858321551080267055879090$

$k := 71$

$p0 := 557940830126698960967415390$

$k := 73$

$p0 := 40729680599249024150621323470$

$k := 79$

$p0 := 3217644767340672907899084554130$

$k := 83$

$p0 := 267064515689275851355624017992790$

$k := 89$

$p0 := 23768741896345550770650537601358310$

$k := 97$

$p0 := 2305567963945518424753102147331756070$

$k := 101$

$p0 := 232862364358497360900063316880507363070$

$k := 103$

$p0 := 23984823528925228172706521638692258396210$

$k := 107$

$p0 := 2566376117594999414479597815340071648394470$

$k := 109$

$p0 := 279734996817854936178276161872067809674997230$

$k := 113$

$p0 := 31610054640417607788145206291543662493274686990$

$k := 127$

$p0 := 4014476939333036189094441199026045136645885247730$

$k := 131$

$p0 := 525896479052627740771371797072411912900610967452630$

$k := 137$

$p0 := 72047817630210000485677936198920432067383702541010310$

$k := 139$

$p0 := 10014646650599190067509233131649940057366334653200433090$

$k := 149$ (3)

> $igcd(10014646650599190067509233131649940057366334653200433090, 20953)$

23 (4)

>

(b) What is the value of P_0 that you need to guarantee finding a factor given that b is composite?

Answer: From the Maple worksheet from 2(a), the P_0 value that guarantee a minimum factor is the product of all primes upto 23 inclusive of 23. Hence the required $P0 = 223092870$

3. Take the number c assigned to you on page and use the $p-1$ method to find one factor of c. You may assume that $c-1$ factorises into primes of $size < 100$.

Answer:

4. Take the number d assigned to you on page and use the $p-1$ method to find both factors of d. You may NOT use the maple procedure provided in weblearn.

Answer:

5. Take the same number d and now factorise using the Quadratic Sieve method. You may use Maple commands included in the week 10 workshop folder.

Answer: $d = 500657$

Step 1. We use the polynomial $y(x) = x^2 - d$ to find the B-smooth numbers. We initialise $x = \sqrt{500657}$ to start the sieve. Calculate the square root of d.
$a = \lfloor\sqrt{500657}\rfloor = 707$
We then $y(x), y(x+1), y(x+2), ...$

Step 2. Calculate the factor base. Euler's criteria for odd primes to determine whether a number is a quadratic residue or not is in action here. We got the below Factor Base: $\{2, 11, 13, 19, 23, 29, 31\}$. We added -1 to it to consider negative values too. Hence the Factor Base became $\{-1, 2, 11, 13, 19, 23, 29, 31\}$

Step 3. Calculate $y(x)$ and sieve the B-smooth numbers. Here we set $B = 7$.

Step 4. the table below shows the sieved numbers and the corresponding exponents matrix (I wrote some Rust code to 1 generate these values.)

x	**y(x + a)**	**-1**	**2**	**11**	**13**	**19**	**23**	**29**	**31**
-97	610	1	0	1	1	0	0	1	1
-82	625	1	4	0	1	0	2	0	0
-31	676	1	0	2	0	2	0	0	0
-12	695	1	5	0	0	1	0	1	0
-10	697	1	9	0	0	0	0	1	0
-4	703	1	4	0	1	0	0	0	1
2	709	0	3	1	0	0	1	0	0
4	711	0	8	0	0	1	0	0	0
46	753	0	4	1	1	0	0	1	0
48	755	0	3	0	1	0	1	1	0
58	765	0	3	1	0	0	0	0	2
61	768	0	0	0	1	3	0	0	0
102	809	0	5	1	0	1	1	0	0
140	847	0	4	0	0	1	1	0	1
178	885	0	3	1	2	1	0	0	0
Selected Rows' sum		2	12	2	2	6	2	0	0
Values for v		1	6	1	1	3	1	0	0

Table 2: Quadratic Sieve Factorisation

Step 5. We calculate v and u as follows:

$$\begin{aligned}
&u = 625 \times 676 \times 711 \times 768 \pmod{500657} \\
&\;= 31115 \\
&v = -1 \times 2^6 \times 11 \times 13 \times 19 \times 23 \pmod{500657} \\
&\;= 102724 \\
&u^2 \equiv v^2 \pmod{500657} \implies gcd(d, u-v) and gcd(d, u+v) are factors of d \\
&gcd(500657, 71609) = 101 \\
&gcd(500657, 133839) = 4957 \\
&\therefore 500657 = 101 \times 4957
\end{aligned}$$

∎

Step 6. The Rust code for generating the above result is below.

```rust

pub fn prepare_matrix(n: &BigInt) {
    let mut primes = vec![BigInt::from(2u64)];
    let a = n.sqrt();
     println!("Square Root of {} = {}", n, a);

    let mut factor_base = vec![
     BigInt::from(2u64),
     BigInt::from(5u64),
     BigInt::from(7u64),
     BigInt::from(11u64),
     BigInt::from(13u64),
     BigInt::from(17u64),
     BigInt::from(19u64),
     BigInt::from(23u64),
     BigInt::from(29u64),
     BigInt::from(31u64),
    ];

     println!("Legendre Symbol is calculated
         using Euler's criteria: ");
     println!("If n^(p-1)/2 (mod p) = 1,
         then (n/p) = 1, else (n/p) = -1");
     factor_base
         .retain(|x| modular_pow(n, &((x - 1) / BigInt::from(2u64)), x) == BigInt::one());
    // factor_base.insert(0, BigInt::from(-1i32));
     println!("The calculated Factor Base is: {:?}", &factor_base);
    let mut y_x: Vec<BigInt> = Vec::new();
    let start = a.clone() - BigInt::from(100u64);
    let end = a.clone() + BigInt::from(200u64);

    let mut m_by_n: Vec<Vec<i32>> = Vec::new();
    for i in range_inclusive(start, end) {
        let x = &i - &a;
        y_x.push(x.clone());
        let mut y = &i * &i - n;
        if y.sign() == Sign::Minus {
            y = -1 * y;
        }
        let p_factors = y.prime_factors(&mut primes).clone();
        let p_factors_map: HashMap<BigInt, i32> = p_factors
        .iter()
        .cloned()
        .map(|(p, e)| (p, e as i32))
        .collect();
        let distinct_factors = p_factors
```

```rust
            .iter()
            .map(|x| x.0.clone())
            .collect::<Vec<BigInt>>();
        let set1: HashSet<BigInt> = factor_base
            .iter().cloned().collect();
        let set2: HashSet<BigInt> = distinct_factors
            .iter().cloned().collect();

        if set2.is_subset(&set1) {
            // println!("{} {} {:?}", i - &a, &y, p_factors);

            let mut one_by_n: Vec<i32> = Vec::new();
            for base in factor_base.iter() {
                if set2.contains(&base) {
                    let e = p_factors_map.get(&base).unwrap();
                    one_by_n.push(e.clone());
                } else {
                    one_by_n.push(0);
                }
            }

            if x.sign() == Sign::Minus {
                one_by_n.insert(0, 1);
            } else {
                one_by_n.insert(0, 0);
            }
            m_by_n.push(one_by_n.clone());
            println!("{:>3} {:>2} {:?}", x, i, one_by_n);
        }
    }
}

```

Listing 1: Quadratic Sieve

We can use the below command to generate the desired matrix:

```
./target/debug/nt-assignments quadratic-sieve -n 500657
Square Root of 500657 = 707
Legendre Symbol is calculated using Euler's criteria:
If n^(p-1)/2 (mod p) = 1, then (n/p) = 1, else (n/p) = -1
The calculated Factor Base is: [2, 11, 13, 19, 23, 29, 31]
-97 610 [1, 0, 1, 1, 0, 0, 1, 1]
-82 625 [1, 4, 0, 1, 0, 2, 0, 0]
-31 676 [1, 0, 2, 0, 2, 0, 0, 0]
-12 695 [1, 5, 0, 0, 1, 0, 1, 0]
-10 697 [1, 9, 0, 0, 0, 0, 1, 0]
-4 703 [1, 4, 0, 1, 0, 0, 0, 1]
2 709 [0, 3, 1, 0, 0, 1, 0, 0]
4 711 [0, 8, 0, 0, 1, 0, 0, 0]
46 753 [0, 4, 1, 1, 0, 0, 1, 0]
48 755 [0, 3, 0, 1, 0, 1, 1, 0]
58 765 [0, 3, 1, 0, 0, 0, 0, 2]
61 768 [0, 0, 0, 1, 3, 0, 0, 0]
102 809 [0, 5, 1, 0, 1, 1, 0, 0]
140 847 [0, 4, 0, 0, 1, 1, 0, 1]
178 885 [0, 3, 1, 2, 1, 0, 0, 0]


./target/debug/nt-assignments gcd-euclid -a 500657 -b 71609
101
./target/debug/nt-assignments gcd-euclid -a 500657 -b 133839
4957

```

Listing 2: Quadratic Sieve Matrix Generation

6. The Maple worksheet in Weblearn for this assignment shows part of an attempt to factorise $N = 9263 = 59 * 157$ using the Number Field Sieve. In this we claim the following:

   i. $A = [0, 1, 0]$ is a prime(irreducible) element of $Z(\sqrt[3]{-2})$ with $norm = 2$

   ii. $B = [-1, -1, 0]$ is a prime(irreducible) element of $Z(\sqrt[3]{-2})$ with $norm = 3$

   iii. $C = [1, 0, 1]$ is a prime(irreducible) element of $Z(\sqrt[3]{-2})$ with $norm = 5$

   iv. $D = [1, 1, -1]$ is a prime(irreducible) element of $Z(\sqrt[3]{-2})$ with $norm = 11$

   v. $E = [1, -2, 0]$ is a prime(irreducible) element of $Z(\sqrt[3]{-2})$ with $norm = 17$

   vi. $F = [3, 0, -1]$ is a prime(irreducible) element of $Z(\sqrt[3]{-2})$ with $norm = 23$

   We also derive a 48×15 matrix R consisting of values of a and b such that $a + 21b$ can be factorised using small primes and $[a, b, 0]$ can be factorised in $Z(\sqrt[3]{-2})$ using just the primes $\{A, B, C, D, E, F\}$ and a unit element $U = [1, 1, 0]$.

   a. Prove the statement above allocated to you on page 1 using the definition of a norm.

   Answer: Norm is defined as the product of all the conjugates of the minimum polynomial in the field. i,e. in the For the polynomial $f(x) = x^3 + 2$, the roots are $\theta = \{\sqrt[3]{-2}, \theta.\frac{(-1+i\sqrt{3})}{2}, \theta.\frac{(-1-i\sqrt{3})}{2}\}$. Hence the algebraic integers in $Z(\sqrt[3]{-2})$ are of the form $a + b\theta + c\theta^2$. We represent these integers as $[a, b, c]$. The norm is defined as:

   $$N[a, b, c] = a^3 - 2b^3 + 4c^3 + 6abc. \quad \text{hence in our case, } [a, b, c] = [-1, -1, 0] \implies N([a, b, c]) = -1 +$$

   Since the $norm = 1$, the given element $B = [-1, -1, 0]$ is a *unit* in $Z(\sqrt[3]{-2})$, not a prime. □

   b. Show that rows 23, 37, 41 and 45 of the matrix form a linearly dependent set modulo 2

   Answer: The rows 23, 37, 41, 45 in matrix form is:

   $$A_{4\times 15} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 3 & 3 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 5 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 9 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

   $$A \pmod 2 \text{ gives, } A = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

   Performing row operations on A to find the Row Echelon form:
   R2 = R2 + R1,
   R3 = R3 + R1,
   R4 = R4 + R1:

   $$B = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

   Swap R2 and R4

   $$B = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

   R3 = R3 + R2

   $$B = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

R3 and R4 are the same, R4 is a linear combination of the row R4. Hence the matrix becomes:

$$B = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Hence the $rank(A) = 3$ (the number of leading 1's in the B) which is less than the number of rows in A and that implies A that the row vectors that form the matrix A are linearly dependent. □

c. Hence find an equation of the form u2 – v2 such that u2 – v2 and N have a common factor of 59 thus factorising N. You may use the Maple procedure for multiplication in $Z(\sqrt[3]{-2})$ to help you find u and v.

Answer:

$N = 9263 = 21^3 + 2$

An elementβ is of the form$(a + b\theta + c\theta^2) \in \mathbb{Z}(\sqrt[3]{-2})$

The Algebraic Factor Base given is $= \{U = [1, 1, 0], A = [0, 1, 0], B = [-1, 1, 0], C = [1, 0, 1], D = [1$

The Rational Factor Base given is $= \{-1, 2, 3, 5, 7, 11, 13\}$

The below table has the values selected for calculating u and v:

a	**b**	**a+21b**	**-1**	**2**	**3**	**5**	**7**	**11**	**13**	**-1**	**U**	**A**	**B**	**C**	**D**	**E**	**F**
0	2	42	0	1	1	0	1	0	0	1	0	4	0	0	0	0	0
6	0	6	0	1	1	0	0	0	0	1	1	3	3	0	0	0	0
7	3	70	0	1	0	1	1	0	0	1	1	0	0	0	0	2	0
-8	8	160	0	5	0	1	0	0	0	1	0	9	1	0	0	0	0
Sum Of Rows			0	10	2	2	2	0	0	4	2	16	4	0	0	2	0

Table 3: Number Field Sieve Factorisation

Calculating the v value by multiplying the rational factor bases with halved values from the Sum Row: $v = 2^5 \times 3 \times 5 \times 7 = 1680$

Calculating the u value by multiplying the algebraic factor bases with halved values from the Sum Row:

$$\begin{aligned} \beta =& [a, b, c] \\ =& U \times A^8 \times B^2 \times E \\ =& [1, 1, 0] \times [0, 1, 0]^8 \times [-1, 1, 0] \times [-1, 1, 0] \times [1, -2, 0] \end{aligned}$$

We get value for u after substituting for a, b, c in $a + b\theta + c\theta^2$ where $\theta = 21$.

$u = -8 + 21 \times -8 + 21^2 \times -20 = -8996$

$u^2 = 6448 \pmod{9263}, u^2 = 6448 \pmod{9263}$

And we get $v^2 \equiv u^2 \pmod{9263}$

Calculating gcd to find the factors:

$$gcd(9263, 1680 + 8996) = 157$$
$$gcd(9263, 1680 - 8996) = 59$$

Hence, N is factorised as $N = 9263 = 59 \times 157$ ■

The Maple calculation performed is given below:

>

> $norm1 := \mathrm{proc}(a, b, c)\,\mathrm{global}\,k;\ k := a^3 - 2 \cdot b^3 + 4 \cdot c^3 + 6 \cdot a \cdot b \cdot c;\mathrm{end};$

$$-10258 \tag{5}$$

> $U := [1, 1, 0]; A := [0, 1, 0]; B := [-1, 1, 0]; C := [1, 0, 1]; D1 := [1, 1, -1]; E := [1, -2, 0]; F := [3, 0, -1];$

$$U := [1, 1, 0]$$

$$A := [0, 1, 0]$$

$$B := [-1, 1, 0]$$

$$C := [1, 0, 1]$$

$$D1 := [1, 1, -1]$$

$$E := [1, -2, 0]$$

$$F := [3, 0, -1] \tag{6}$$

> $mult1 := \mathrm{proc}(x, y);\ mult2(x[1], x[2], x[3], y[1], y[2], y[3])\,;\mathrm{end};$
> $mult4 := \mathrm{proc}()\mathrm{global}\,L;\ L := [];\ \mathrm{for}\,i\,\mathrm{from}\,1\,\mathrm{to}\,nargs$
$\mathrm{do}\,L := [op(L), args[i]];\mathrm{od};$
$\mathrm{if}\,nops(L) = 2\,\mathrm{then}$
$mult1(op(1, L), op(2, L))\,\mathrm{else}\,k := [mult1(op(1, L), op(2, L))]; L$
$:= subsop(1 = NULL, L);\ L := subsop(1 = NULL, L); L := [k, op(L)];\ mult4(op(L));\mathrm{fi};\mathrm{end};$
> $mult4(U, U, B, E);$

$$1, 5, 3 \tag{7}$$

> $H := mult4(U, A, A, A);$

$$H := -2, -2, 0 \tag{8}$$

>
> $H := [-2, -2, 0];$

$$H := [-2, -2, 0] \tag{9}$$

> $mult4(H, A, A, A);$

$$4, 4, 0 \tag{10}$$

> $H := [4, 4, 0];$

$$H := [4, 4, 0] \tag{11}$$

> $mult4(H, A, A, B);$

$$0, -8, -4 \tag{12}$$

> $H := [0, -8, -4];$

$$H := [0, -8, -4] \tag{13}$$

> $mult4(U, H, B, E)$;

$$32, -16, -28 \tag{14}$$

> $M := mult1(0, -8, -4, -1, 1, 0)$;

$$M := 0, 0, 0 \tag{15}$$

> $mult1(0, 0, 0, 1, -2, 0)$;

$$0, 0, 0 \tag{16}$$

>

U*A^8*B^2*E $= [1, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [0, 1, 0] \cdot [-1, 1, 0] \cdot [-1, 1, 0] \cdot [1, -2, 0]$;

>

> $mult1(U, A)$;

$$0, 1, 1 \tag{17}$$

> $UA := [0, 1, 1]$;

$$UA := [0, 1, 1] \tag{18}$$

> $mult1(UA, A)$;

$$-2, 0, 1 \tag{19}$$

> $UAA := [-2, 0, 1]$;

$$UAA := [-2, 0, 1] \tag{20}$$

> $mult1(UAA, A)$;

$$-2, -2, 0 \tag{21}$$

> $UAAA := [-2, -2, 0]$;

$$UAAA := [-2, -2, 0] \tag{22}$$

> $mult1(UAAA, A)$;

$$0, -2, -2 \tag{23}$$

> $UAAAA := [0, -2, -2]$;

$$UAAAA := [0, -2, -2] \tag{24}$$

> $mult4(UAAAA, A, A, A)$;

$$0, 4, 4 \tag{25}$$

> $UAAAAAAA := [0,4,4];$

$$UAAAAAAA := [0,4,4] \tag{26}$$

> $mult4(UAAAAAAA, A);$

$$-8, 0, 4 \tag{27}$$

> $UA8 := [-8,0,4];$

$$UA8 := [-8,0,4] \tag{28}$$

> $mult4(UA8, B, B, E);$

$$-8, -8, -20 \tag{29}$$

>
u = phi(a + bz + cz^2) = a + 21b + 21^2c = -8 + 21*-8 + 21^2 * -20 = -8996 v = 2^4*3*5*7 = 1680 v^2 mod 9263 = 6448
u^2 mod 9263 = 6448
gcd(9263, 1680 + 8996) = 157
gcd(9263, 1680 - 8996) = 59
> $igcd(9263, 10676);$

$$157 \tag{30}$$

> $igcd(9263, 7316);$

$$59 \tag{31}$$

> $ifactor(9263);$

$$(59)\,(157) \tag{32}$$

7. Compare the methods for integer factorisation you have seen in the module and summarises their strengths and weaknesses, including the size of numbers that can be factorised, usability and whether or not they work for a broad range of numbers.

References

[1] C R Jordan & D A Jordan *MODULAR MATHEMATICS Groups* .

[2] Dr. Ben Fairbairn *GROUP THEORY Solutions to Exercises.*

[3] *https://github.com/Ssophoclis/AKS-algorithm/blob/master/AKS.py*