FOURTH LECTURE FOR THE RESEARCH SCHOOL CIMPA 2015: "PRIMALITY AND FACTORIZATION"

DANIEL C. MAYER

1. Primality testing

1.1. Pseudoprimes and Carmichael Numbers.

Theorem 1.1. ***(Little Fermat).***
If p is a prime number, then $a^{p-1} \equiv 1 \pmod{p}$ for all residues $1 \leq a \leq p-1$.

Motivated by Fermat's Little Theorem, we define:

Definition 1.1. Let $m > 1$ be an integer and let $1 < a < m$ be a coprime residue with $\gcd(a, m) = 1$. Then m is called a *probable prime to base a* if $a^{m-1} \equiv 1 \pmod{m}$.

However, the Fermat Theorem is not reversible, since there exist composite numbers m which are probable primes to a coprime base a.

Definition 1.2. Let $m > 1$ be a *composite* integer and let $1 < a < m$ be a coprime residue with $\gcd(a, m) = 1$. Then m is called a *pseudoprime to base a* if $a^{m-1} \equiv 1 \pmod{m}$.

Example 1.1. The *smallest pseudoprime to base $a = 2$* is $m = 341$, since

$$2^{10} - 1 = 1024 - 1 = 1023 = 3 \cdot 341$$

and thus we have $2^{10} \equiv 1 \pmod{341}$ and consequently

$$2^{m-1} = 2^{340} = (2^{10})^{34} \equiv 1 \pmod{341}.$$

However, since the alternating digit sum of m is $3 - 4 + 1 = 0$, we conclude that $11 \mid m$. Indeed, $m = 341 = 11 \cdot 31$ is composite.

Date: March 18, 2015.
2000 *Mathematics Subject Classification.* Primary 11Y40, 11Y65, 14H52, 14K22; 11R37, 11R29, 11R11, 11R16, 11R20; Secondary 11Y11, 11Y05; 20D15, 20F12, 20F14.
Key words and phrases. algebraic number theory computations, continued fractions, elliptic curves, complex multiplication, primality, factorization; p-class field towers, maximal unramified pro-p extensions, second and higher p-class groups, principalization of p-classes, quadratic fields, cubic fields, quartic fields, quintic fields, dihedral fields, Frobenius fields, finite p-groups, coclass graphs, pro-p groups, Artin transfers, p-covering group, p-multiplier, nucleus, relation rank, generator rank, balanced groups, inversion automorphism, Schur σ-groups, annihilator ideals, commutator calculus, central series.

Remark 1.1. Since $(a_n)_{n\geq 1}$ with $a_n = 2^n - 1$ is a *divisibility sequence*, having the property that $k \mid n \Longrightarrow a_k \mid a_n$, we could have found the complete factorization of 1023 more quickly: since 2 and 5 both divide 10, we conclude that both, $2^2 - 1 = 3$ and $2^5 - 1 = 31$, divide $2^{10} - 1 = 1023$.

Even worse, primality cannot be forced by requiring the Fermat congruence for several distinct bases:

Definition 1.3. Let $m > 1$ be an *odd composite* integer. Then m is called an *absolute pseudoprime* or *Carmichael number* if $a^{m-1} \equiv 1 \pmod{m}$ for every residue $1 < a < m$ which is coprime with $\gcd(a, m) = 1$.

Example 1.2. The *smallest Carmichael number* is $m = 561 = 3 \cdot 187 = 3 \cdot 11 \cdot 17$, since the *exponent* of the *prime residue class group* $U(\mathbb{Z}/m\mathbb{Z})$ is given by

$$\Lambda(m) = \operatorname{lcm}(3-1, 11-1, 17-1) = \operatorname{lcm}(2, 10, 16) = \operatorname{lcm}(2, 2 \cdot 5, 2^4) = 2^4 \cdot 5 = 80$$

and consequently

$$a^{m-1} = a^{560} = (a^{80})^7 \equiv 1 \pmod{561}$$

for all $1 < a < m$ with $\gcd(a, m) = 1$.

Definition 1.4. Let $m > 1$ be an integer and let $1 < a < m$ be a coprime residue with $\gcd(a, m) = 1$. Then m is called a *strong probable prime to base* a if $m - 1 = 2^e \cdot f$ with *odd* factor f implies either $a^f \equiv 1 \pmod{m}$ or $a^{f \cdot 2^c} \equiv -1 \pmod{m}$ for some $0 \leq c < e$.
If additionally m is *composite*, then m is called a *strong pseudoprime to base* a.

Example 1.3. The *smallest strong pseudoprime to base* $a = 2$ is $m = 2047$, since

$$2^{11} - 1 = 2048 - 1 = 2047$$

and thus we have $2^{11} \equiv 1 \pmod{2047}$. Further,

$$m - 1 = 2046 = 2 \cdot 1023 = 2 \cdot 3 \cdot 11 \cdot 31,$$

according to Example 1.1, whence $e = 1$, $f = 1023$, and consequently

$$2^f = 2^{1023} = (2^{11})^{93} \equiv 1 \pmod{2047}.$$

However, $m = 2047 = 23 \cdot 89$ is composite, since $p = 11 \equiv 3 \pmod{4}$,

$$q = 2p + 1 = 23 \equiv 7 \pmod{8}$$

is *prime*, and consequently $\left(\frac{2}{q}\right) = 1$, and $2^p = 2^{\frac{q-1}{2}} \equiv 1 \pmod{q}$, by the *Euler criterion* for the quadratic residue 2 modulo q.

1.2. **Primality Tests.** Let $p \geq 3$ be an odd prime. Denote by $M_p := 2^p - 1$ the *Mersenne number* with exponent p.

Definition 1.5. The *Lucas sequence* $(L_n)_{n\geq 0}$ is defined recursively by

$$L_0 := 4 \quad \text{and} \quad L_n := L_{n-1}^2 - 2 \text{ for } n \geq 1.$$

Proposition 1.1. *Let $\varepsilon = 2 + \sqrt{3} > 1$ and $0 < \bar{\varepsilon} = 2 - \sqrt{3} < 1$ be the fundamental unit of $\mathbb{Q}(\sqrt{3})$ and its inverse.*
The terms of the Lucas sequence can be represented in the form $L_n = \varepsilon^{2^n} + \bar{\varepsilon}^{2^n}$ for all $n \geq 0$.

Proof. For $n = 0$, we have the correct initialization $L_0 = \varepsilon^{2^0} + \bar{\varepsilon}^{2^0} = \varepsilon + \bar{\varepsilon} = 2 + \sqrt{3} + 2 - \sqrt{3} = 4$. By induction, if $L_{n-1} = \varepsilon^{2^{n-1}} + \bar{\varepsilon}^{2^{n-1}}$ for some $n \geq 1$, then $L_{n-1}^2 = (\varepsilon^{2^{n-1}} + \bar{\varepsilon}^{2^{n-1}})^2 = \varepsilon^{2^n} + 2\varepsilon^{2^{n-1}}\bar{\varepsilon}^{2^{n-1}} + \bar{\varepsilon}^{2^n} = L_n + 2$, since $\mathrm{Norm}(\varepsilon) = \varepsilon\bar{\varepsilon} = 2^2 - 3 = +1$, and the desired recursion formula $L_n = L_{n-1}^2 - 2$ is satisfied. □

Theorem 1.2. *(D.H. Lehmer, 1930)*
The Mersenne number $M_p = 2^p - 1$ with odd prime exponent p is prime if and only if it divides the $(p-2)$th term of the Lucas sequence, $L_{p-2} \equiv 0 \pmod{M_p}$.

Proof. (by Rosen and Bruce)

- Necessity:
  If $M_p = 2^p - 1$ is prime, then we put $q := M_p$. According to the binomial formula, we have
  $$(1 + \sqrt{3})^q = \sum_{i=0}^{q} \binom{q}{i} (\sqrt{3})^i \equiv 1 + (\sqrt{3})^q \pmod{q},$$
  since the binomial coefficients $\binom{q}{i}$ are divisible by q for $1 \leq i \leq q-1$. Here, we can write
  $$(\sqrt{3})^q = \sqrt{3} \cdot (\sqrt{3})^{q-1} = \sqrt{3} \cdot 3^{\frac{q-1}{2}}.$$
  Since p is odd and $2 \equiv -1 \pmod 3$, we have $2^p \equiv (-1)^p = -1 \pmod 3$, and consequently $q = 2^p - 1 \equiv -2 \equiv 1 \pmod 3$, whence $\left(\frac{q}{3}\right) = +1$. Since both, 3 and $q = 2^p - 1$ are $\equiv -1 \pmod 4$, the law of quadratic reciprocity implies that $\left(\frac{3}{q}\right) = -1$, and by the Euler criterion, we have $3^{\frac{q-1}{2}} \equiv -1 \pmod q$. Thus
  $$(1 + \sqrt{3})^q \equiv 1 + \sqrt{3} \cdot 3^{\frac{q-1}{2}} \equiv 1 - \sqrt{3} \pmod q$$
  and multiplication by $1 + \sqrt{3}$ yields
  $$(1 + \sqrt{3})^{q+1} \equiv 1^2 - 3 = -2 \pmod q.$$
  Further, we have
  $$(1 + \sqrt{3})^2 = 1 + 2\sqrt{3} + 3 = 4 + 2\sqrt{3} = 2 \cdot (2 + \sqrt{3}) = 2\varepsilon$$

and thus

$$(1+\sqrt{3})^{q+1} = (2\varepsilon)^{\frac{q+1}{2}} \equiv -2 \pmod{q},$$

where

$$(2\varepsilon)^{\frac{q+1}{2}} = 2^{\frac{q+1}{2}} \cdot \varepsilon^{\frac{q+1}{2}} = 2 \cdot 2^{\frac{q-1}{2}} \cdot \varepsilon^{\frac{q+1}{2}}.$$

The second supplement to the quadratic reciprocity law implies that $\left(\frac{2}{q}\right) = +1$, since $q = M_p = 2^p - 1$ with $p \geq 3$, i.e. $q \equiv -1 \pmod 8$, and the Euler criterion states that $2^{\frac{q-1}{2}} \equiv 1 \pmod{q}$, whence $2 \cdot \varepsilon^{\frac{q+1}{2}} \equiv -2 \pmod{q}$. Since $\frac{q+1}{2} \cdot 2 = q+1 \equiv 1 \pmod{q}$, the integer $\frac{q+1}{2}$ is the multiplicative inverse of 2. By multiplication with $\frac{q+1}{2}$, we obtain $\varepsilon^{\frac{q+1}{2}} \equiv -1 \pmod{q}$, where $\varepsilon^{\frac{q+1}{2}} = \varepsilon^{\frac{2^p}{2}} = \varepsilon^{2^{p-1}} = \varepsilon^{2^{p-2}} \cdot \varepsilon^{2^{p-2}}$. Multiplying by $\bar{\varepsilon}^{2^{p-2}}$ yields $\varepsilon^{2^{p-2}} \equiv -\bar{\varepsilon}^{2^{p-2}} \pmod{q}$, resp. $L_{p-2} = \varepsilon^{2^{p-2}} + \bar{\varepsilon}^{2^{p-2}} \equiv 0 \pmod{q}$ with $q = M_p$.

- Sufficiency:

  Suppose that $L_{p-2} \equiv 0 \pmod{M_p}$ but $M_p = 2^p - 1$ were not prime. Then it had a prime factor $q \leq \sqrt{M_p}$. The hypothesis implies $\varepsilon^{2^{p-2}} + \bar{\varepsilon}^{2^{p-2}} = L_{p-2} = mq$ for some integer m. Multiplication by $\varepsilon^{2^{p-2}}$ yields $\varepsilon^{2^{p-1}} = mq\varepsilon^{2^{p-2}} - 1$, since $\varepsilon\bar{\varepsilon} = 1$. Forming the squares, we obtain $\varepsilon^{2^p} = (mq\varepsilon^{2^{p-2}} - 1)^2$. Now we consider these equations in the ring $(\mathbb{Z} \oplus \mathbb{Z}\sqrt{3})/q\mathbb{Z}$ of cardinality q^2 with unit group $U := U((\mathbb{Z}/q\mathbb{Z}) \oplus (\mathbb{Z}/q\mathbb{Z})\sqrt{3})$ of order $\mathrm{ord}(U) \leq q^2 - 1$ (since 0 is not invertible),

  $$\varepsilon^{2^{p-1}} \equiv -1 \pmod{q} \quad \text{but} \quad \varepsilon^{2^p} \equiv (-1)^2 = 1 \pmod{q},$$

  and therefore the order of ε in this unit group is

  $$2^p = \mathrm{ord}(\varepsilon) \leq \mathrm{ord}(U) \leq q^2 - 1 \leq M_p - 1 = 2^p - 2,$$

  which gives the contradiction $0 \leq -2$. Consequently, M_p must be prime.

□

1.3. **Sieving Algorithms.**

Algorithm 1.1. (Basic Sieve of Eratosthenes)
Input: a given positive integer B as an upper bound.
Memory: an array $P[j]$, $1 \leq j \leq B$, of bits.
Initialization:
$P[1] \leftarrow 0$;
`for` $(j \leftarrow 2 \dots B)$ $\{P[j] \leftarrow 1;\}$
$p \leftarrow 2$;
Recursion:
`while` $(p \leq \sqrt{B})$ {
    $j \leftarrow p \cdot p$;
    `while` $(j \leq B)$ $\{P[j] \leftarrow 0;\ j \leftarrow j + p;\}$
    $j \leftarrow p + 1$;
    `while` $(j \leq \sqrt{B}$ `and` $P[j] = 0)$ $\{j \leftarrow j + 1;\}$
    $p \leftarrow j$;
}
Termination: $p > \sqrt{B}$.
Output:
a list of all primes $p \leq B$ in the array P such that
for each $1 \leq j \leq B$, we have: j prime $\Longleftrightarrow P[j] = 1$.
Complexity: $O(B \log \log B)$ steps.

2. Factoring large integers

2.1. **A general plan for factoring.**

Theorem 2.1. *If $N > 1$ is a composite integer and x, y are integers such that*

$$\begin{aligned} x^2 &\equiv y^2 \pmod{N}, \\ x &\not\equiv \pm y \pmod{N}, \end{aligned} \tag{1}$$

then $\gcd(x-y, N)$ *and* $\gcd(x+y, N)$ *are proper factors of* N*.*

Proof. If $x \not\equiv \pm y \pmod{N}$, that is $N \not| (x-y)$ and $N \not| (x+y)$, then there exist prime divisors p and q of N such that $p \not| (x-y)$ and $q \not| (x+y)$. However, the condition $x^2 \equiv y^2 \pmod{N}$, that is $N|(x^2-y^2) = (x+y)(x-y)$, together with $p|N$ and $q|N$, implies $p|(x+y)$ and $q|(x-y)$ and thus $p|\gcd(x+y, N)$ and $q|\gcd(x-y, N)$. Finally, $\gcd(x-y, N)$ and $\gcd(x+y, N)$ must be proper factors of N, since $\gcd(x-y, N) = N$ would imply $N|(x-y)$ and $\gcd(x+y, N) = N$ would imply $N|(x+y)$, which are both contradictions. □

Theorem 2.2. *If $N > 1$ is an odd integer with at least $\omega(N) \geq 2$ prime divisors and two integers x, y are selected randomly such that $x^2 \equiv y^2 \pmod{N}$, then $\gcd(x-y, N)$is a proper factor of N with probability at least $\frac{1}{2}$.*

Proof. Let $k := \omega(N)$ and $N = p_1^{e_1} \cdots p_k^{e_k}$ be the prime decomposition of N.
If $x^2 \equiv y^2 \pmod{N}$, then $x^2 \equiv y^2 \pmod{p_i^{e_i}}$, for each $1 \leq i \leq k$.
Since each congruence $T^2 \equiv y^2 \pmod{p_i^{e_i}}$ has 2 solutions, y and $-y$, there are 2^k solutions to $T^2 \equiv y^2 \pmod{N}$, for a given y, by the Chinese Remainder Theorem. Two of them are $x \equiv \pm y \pmod{N}$. Therefore, the probability that $x \not\equiv \pm y \pmod{N}$, for randomly selected integers x, y subject to $x^2 \equiv y^2 \pmod{N}$, is given by the fraction $\frac{2^k-2}{2^k} = 1 - \frac{1}{2^{k-1}}$, where $k \geq 2$, $2^{k-1} \geq 2$, $\frac{1}{2^{k-1}} \leq \frac{1}{2}$, and consequently $1 - \frac{1}{2^{k-1}} \geq 1 - \frac{1}{2} = \frac{1}{2}$. □

Corollary 2.2.1. *Let $N > 1$ be an odd integer with at least $\omega(N) \geq 2$ prime divisors. If there is a probabilistic polynomial time algorithm $\mathcal{A}$ to find a solution to $T^2 \equiv r \pmod{N}$ for any quadratic residue r modulo N, then there is a probabilistic polynomial time algorithm $\mathcal{B}$ to find a factor of N.*

Proof. Algorithm $\mathcal{B}$: Select a random $0 < y < N$. If $d := \gcd(y, N) > 1$ then d is a proper factor of N. If $d = 1$, then $r := y^2 \pmod{N}$ is a quadratic residue modulo N. Now call algorithm $\mathcal{A}$ with input r. If $\mathcal{A}$ returns with output y or $N - y$, then repeat the above steps with a new random y. Otherwise, let x be the output of $\mathcal{A}$. Then $\gcd(x-y, N)$ is a proper factor of N, by Theorem 2.1. According to Theorem 2.2, the probability of success for each random y is at least $\frac{1}{2}$. □

2.2. **Factoring with continued fractions.** The basic idea in the following subexponential factoring algorithm is to use the steps of the continued fraction expansion of N for constructing quadratic congruences $x^2 \equiv y^2 \pmod N$ as needed in Theorem 2.1. It goes back to Kraitchik in 1929, and Lehmer / Powers in 1931. However the restriction to a fixed factor base and the Gaussian elimination modulo 2 is due to Brillhart / Morrison in 1975.

Algorithm 2.1. (Continued Fraction Integer Factoring Algorithm)
Input: a composite positive integer N, and an upper bound B for the factor base.
Initialization:
$p_0 \leftarrow -1$;
$K \in \mathbb{N}$ such that $p_1, \ldots, p_K \le B$ are all primes with $\left(\frac{N}{p_i}\right) = +1$;
$R \leftarrow 0$;
$i \leftarrow 0$;
Loop:

`while` $(R < K + 10)$ {
    compute $M_i, N_i, a_i, P_{i-1} \mod N$ using Dfn.1.2 and Thm.1.3 (1st lecture) ;
    try to factor N_i on the factor base $\{p_0, p_1, \ldots, p_K\}$;
    `if` successful `then` {
        store i, N_i, P_{i-1} in a file;
        $R \leftarrow R + 1$;
    }
    $i \leftarrow i + 1$;
}
`for all` i {
    read i, N_i, P_{i-1} from the file;
    factor $(-1)^i N_i = p_0^{e_{i0}} \cdot p_1^{e_{i1}} \cdots p_K^{e_{iK}}$;
    define the row vector $\vec{v}_i \leftarrow (e_{i0}, e_{i1}, \ldots, e_{iK})$;
}
form the matrix with row vectors $\vec{v}_0, \vec{v}_1, \ldots$;
use linear algebra to find dependencies $\sum_{i \in S} \vec{v}_i \equiv \vec{0} \pmod 2$;
`for each` dependency {
    let $y^2 = \prod_{i \in S} (-1)^i N_i$ and $x = \prod_{i \in S} P_{i-1} \mod N$;
    `if` $\gcd(x - y, N)$ is a proper factor of N `then` {
        write the factor;
        STOP;
    }
}

Output: a factor of N.
Complexity: subexponential.

Example 2.1. Use the CFRAC Algorithm 2.1 to find the prime decomposition of the last (and biggest) factor in the product representation

$$s^{53}(276) = 254\,903\,331\,620 = 2^2 \cdot 5 \cdot 7 \cdot 137 \cdot 13\,290\,059$$

of the 53rd term of the aliquot sequence of 276, which was given by D. H. Lehmer in 1931. Select the set $\{-1, 2, 5, 31, 43, 53, 113\}$ as a factor base.

We use the following Magma script to find the CFE of $N = 13\,290\,059$.

```
intrinsic CmplQuot(iRad::RngIntElt,iLen::RngIntElt,iPrc::RngIntElt,bLM::RngIntElt){}
D := iRad; // radicand
printf "D=%8o, (D/p)=1 for p=",D;
for p in [2..120] do
   if (IsPrime(p) and (1 eq KroneckerSymbol(D,p))) then
      printf "%o, ",p;
   end if; // if p prime and D quadratic residue
end for; // for p
printf "\n";
R := RealField(iPrc); // precision of real numbers
d := R!D;
if ((1 eq bLM) and (1 eq D mod 4)) then
   m0 := -1;
   n0 := 2;
   s := R!((-1+Exp(Log(d)/2))/2);
else
   m0 := 0;
   n0 := 1;
   s := R!Exp(Log(d)/2); // quadratic surd
end if; // parity
```

```
a := ContinuedFraction(s: Bound := 10); // partial quotients of CFE

m := a[1]*n0 - m0; // initialization of total quotients
n := (D - m^2) div n0; // for periodic CFE of s

for i in [1..iLen+1] do
   printf "i=%3o",i-1;
   a := ContinuedFraction(s: Bound := i);
   c := Convergents(a); // convergents for CFE of s
   ci := c[1][2];
   printf ", a=%4o",a[i];
   printf ", P mod D=%8o",ci mod D; // numerators
   a := ContinuedFraction(s: Bound := i+1);
   m2 := a[i+1]*n - m; // recursion
   n2 :=  n0 + (m - m2)*a[i+1];
   printf ", M=%4o",m0; // coefficients
   printf ", N=%4o",n0; // denominators
   printf "=%o;\n",Factorization(n0); // factorization
   m0 := m; // permutation
   m := m2;
   n0 := n;
   n := n2;
end for; // for i

end intrinsic; // CmplQuot
```

TABLE 1. Continued fraction expansion of $\sqrt{N}$ for $N = 13\,290\,059$

i	a_i	M_i	N_i	factorized	$(-1)^i$	$P_{i-1} \mod N$
0	3645	0	1		$+1$	1
1	1	3645	4034	$= 2 \cdot 2017$	-1	3 645
2	1	389	3257		$+1$	3 646
3	4	2868	1555	$= 5 \cdot 311$	-1	7 291
4	5	3352	1321		$+1$	32 810
5	3	3253	2050	$= 2 \cdot 5^2 \cdot 41$	-1	171 341
6	2	2897	2389		$+1$	546 833
7	1	1881	4082	$= 2 \cdot 13 \cdot 157$	-1	1 265 007
8	2	2201	2069		$+1$	1 811 840
9	1	1937	4610	$= 2 \cdot 5 \cdot 461$	-1	4 888 687
10	4	2673	1333	$= 31 \cdot 43$	$+1$	6 700 527
11	1	2659	4666	$= 2 \cdot 2333$	-1	5 110 677
12	2	2007	1985	$= 5 \cdot 397$	$+1$	11 811 204
13	1	1963	4754	$= 2 \cdot 2377$	-1	2 152 967
14	5	2791	1157	$= 13 \cdot 89$	$+1$	674 112
15	1	2994	3739		-1	5 523 527
16	1	745	3406	$= 2 \cdot 13 \cdot 131$	$+1$	6 197 639
17	3	2661	1823		-1	11 721 166
18	2	2808	2965	$= 5 \cdot 593$	$+1$	1 490 960
19	5	3122	1195	$= 5 \cdot 239$	-1	1 413 027
20	1	2853	4310	$= 2 \cdot 5 \cdot 431$	$+1$	8 556 095
21	1	1457	2591		-1	9 969 122
22	1	1134	4633	$= 41 \cdot 113$	$+1$	5 235 158
23	31	3499	226	$= 2 \cdot 113$	-1	1 914 221
24	1	3507	4385	$= 5 \cdot 877$	$+1$	11 415 773
25	1	878	2855	$= 5 \cdot 571$	-1	39 935
26	1	1977	3286	$= 2 \cdot 31 \cdot 53$	$+1$	11 455 708
27	1	1309	3523	$= 13 \cdot 271$	-1	11 495 643
28	2	2214	2381		$+1$	9 661 292
29	2	2548	2855	$= 5 \cdot 571$	-1	4 238 109
30	5	3162	1153		$+1$	4 847 451
31	1	2603	5650	$= 2 \cdot 5^2 \cdot 113$	-1	1 895 246
32	9	3047	709		$+1$	6 742 697
33	2	3334	3067		-1	9 419 283
34	3	2800	1777		$+1$	12 291 204
35	1	2531	3874	$= 2 \cdot 13 \cdot 149$	-1	6 422 718
36	1	1343	2965	$= 5 \cdot 593$	$+1$	5 423 863
37	1	1622	3595	$= 5 \cdot 719$	-1	11 846 581
38	2	1973	2614	$= 2 \cdot 1307$	$+1$	3 980 385
39	6	3255	1031		-1	6 517 292
40	1	2931	4558	$= 2 \cdot 43 \cdot 53$	$+1$	3 213 960

TABLE 2. Linear dependencies among the row vectors $\vec{v}_i$

i	-1	2	5	31	43	53	113
10	0	0	0	1	1	0	0
23	1	1	0	0	0	0	1
26	0	1	0	1	0	1	0
31	1	1	2	0	0	0	1
40	0	1	0	0	1	1	0

The first dependency, $\vec{v}_{10} + \vec{v}_{26} + \vec{v}_{40} \equiv \vec{0} \pmod 2$, yields

$$(6\,700\,527 \cdot 11\,455\,708 \cdot 3\,213\,960)^2 \equiv (2 \cdot 31 \cdot 43 \cdot 53)^2 \pmod N$$

and fails, since we obtain $141\,298^2 \equiv 141\,298^2 \pmod N$.
The second dependency $\vec{v}_{23} + \vec{v}_{31} \equiv \vec{0} \pmod 2$, where $2 \equiv 0 \pmod 2$ in $\vec{v}_{31}$, yields

$$(1\,914\,221 \cdot 1\,895\,246)^2 \equiv (-1 \cdot 2 \cdot 5 \cdot 113)^2 \pmod N$$

and succeeds, since we get $12\,677\,605^2 \equiv 1\,130^2 \pmod N$ and thus

$$\gcd(12\,677\,605 - 1\,130, N) = \gcd(12\,676\,475, N) = 4\,261,$$

$$\gcd(12\,677\,605 + 1\,130, N) = \gcd(12\,678\,735, N) = 3\,119.$$

Finally, the *factorization* is $13\,290\,059 = 3\,119 \cdot 4\,261$.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[2] W. Bosma, J. J. Cannon, C. Fieker, and A. Steels (eds.), *Handbook of Magma functions* (Edition 2.21, Sydney, 2015).

[3] H. Cohen, *A course in computational algebraic number theory*, Graduate texts in mathematics **138**, Springer, 1996.

[4] H. Cohen, *Advanced topics in computational number theory*, Graduate texts in mathematics **193**, Springer, 2000.

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming — a System for Computational Discrete Algebra*, Version 4.7.7, Aachen, Braunschweig, Fort Collins, St. Andrews, 2015, (`http://www.gap-system.org`).

[6] The MAGMA Group, *MAGMA Computational Algebra System*, Version 2.21-3, Sydney, 2015, (`http://magma.maths.usyd.edu.au`).

[7] Oracle, *JDK* 7u80, *Java SE*, and *NetBeans*, Version 8.0.2, Redwood City, CA, 2015, (`http://www.oracle.com`).

[8] The PARI Group, *PARI/GP*, Version 2.7.3, Bordeaux, 2015, (`http://pari.math.u-bordeaux.fr`).

[9] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of mathematics and its applications, Cambridge University Press, 1990.

[10] S.S. Wagstaff, Jr., *The Joy of Factoring*, Student Mathematical Library (STML), Vol. **68**, American Mathematical Society (AMS), 2013.

Naglergasse 53, 8010 Graz, Austria

E-mail address: `algebraic.number.theory@algebra.at`

URL: `http://www.algebra.at`