MA503: Homework 3

You can use specialized software (e.g., wolfram alpha) to compute remainders of division and gcd's. Remainders can be computed by google, e.g., search '620^2 % 377753'.

Exercise 3.1. [5pts] Show that $n = 1105$ is a Carmichael number.

Solution: $n = 1105 = 5 \cdot 13 \cdot 17$ and hence it is composite. Pick any a coprime with n. By Fermat little theorem

$$\begin{array}{lcl} a^4 \equiv_5 1 & & a^{1104} \equiv_5 1 & & \\ a^{12} \equiv_{13} 1 & \Rightarrow & a^{1104} \equiv_{13} 1 & \Rightarrow & a^{1104} \equiv_{1105} 1. \\ a^{16} \equiv_{17} 1 & & a^{1104} \equiv_{17} 1 & & \end{array}$$

Hence, $a^{n-1} \equiv_n 1$ and n is Carmichael. □

Exercise 3.2. [5pts] Use base-2 Miller–Rabin primality test to show that $N = 341$ is composite.

Solution: $N - 1 = 340 = 2^2 \cdot 85$ and

$$\begin{aligned} 2^{85} &\equiv_{341} 32, \\ 2^{2 \cdot 85} &\equiv_{341} 1, \\ 2^{4 \cdot 85} &\equiv_{341} 1. \end{aligned}$$

Hence, the algorithm outputs No. □

Exercise 3.3. [10pts] For $N = 6994241$ use Pollard's $p - 1$ algorithm with $a = 2$ to find a non-trivial factor (less than ten iterations will be enough).

Solution:

$$\begin{array}{ll} 2^{1!} \equiv_N 2 & \gcd(2^{1!} - 1, 6994241) = 1, \\ 2^{2!} \equiv_N 4 & \gcd(2^{2!} - 1, 6994241) = 1, \\ 2^{3!} \equiv_N 64 & \gcd(2^{3!} - 1, 6994241) = 1, \\ 2^{4!} \equiv_N 2788734 & \gcd(2^{4!} - 1, 6994241) = 1, \\ 2^{5!} \equiv_N 3834705 & \gcd(2^{5!} - 1, 6994241) = 1, \\ 2^{6!} \equiv_N 513770 & \gcd(2^{6!} - 1, 6994241) = 1, \\ 2^{7!} \equiv_N 443653 & \gcd(2^{7!} - 1, 6994241) = 3361. \end{array}$$

Hence, $p = 3361$ is a non-trivial factor of N obtained on 7th iteration. □

Exercise 3.4. [10pts] Let $N = 377753$. Given the relations

$$\begin{aligned} 620^2 &\equiv_N 6647 = 17^2 \cdot 23, \\ 621^2 &\equiv_N 7888 = 2^4 \cdot 17 \cdot 29 \\ 645^2 &\equiv_N 38272 = 2^7 \cdot 13 \cdot 23 \\ 655^2 &\equiv_N 51272 = 2^3 \cdot 13 \cdot 17 \cdot 29, \end{aligned}$$

find a, b satisfying $a^2 \equiv_N b^2$ and compute $\gcd(a - b, N)$.

Solution: Taking the product for the given identities we obtain

$$(620 \cdot 621 \cdot 645 \cdot 655)^2 \equiv_N 2^{14} \cdot 13^2 \cdot 17^4 \cdot 23^2 \cdot 29^2$$

Then we can define a and b as follows:

$$\begin{aligned} 620 \cdot 621 \cdot 645 \cdot 655 \equiv_N &= 127194 = a, \\ 2^7 \cdot 13 \cdot 17^2 \cdot 23 \cdot 29 \equiv_N &= 45335 = b. \end{aligned}$$

Finally, compute $\gcd(127194 - 45335, 377753) = 751$ which is a non-trivial factor in N. □

Exercise 3.5. [10pts] For $N = 1111$, $f(x) = x^2 + 1$, and $x_1 = 5$ run four iterations (compute four gcds) of the Pollard's rho algorithm and get a non-trivial factor of N.

Solution: Compute some x_i's

$$\begin{array}{llll} x_1 = 5 & x_3 = 677 & x_5 = 974 & x_7 = 358 \\ x_2 = 26 & x_4 = 598 & x_6 = 994 & x_8 = 400 \end{array}$$

and then take gcd's

$$\begin{aligned} \gcd(x_2 - x_1, 1111) &= \gcd(26 - 5, 1111) = 1, \\ \gcd(x_4 - x_2, 1111) &= \gcd(598 - 26, 1111) = 11, \\ \gcd(x_6 - x_3, 1111) &= \gcd(994 - 677, 1111) = 1, \\ \gcd(x_8 - x_4, 1111) &= \gcd(400 - 598, 1111) = 11. \end{aligned}$$

Hence, we could stop the algorithm after getting $\gcd(598 - 26, 1111) = 11$ which is a non-trivial factor in N. $\square$

Definition 3.1. An **integer matrix** is in **row echelon form** if

(1) all nonzero rows (rows with at least one nonzero element) are above any rows of all zeroes (all zero rows, if any, belong at the bottom of the matrix), and
(2) the **leading coefficient** (the first nonzero number from the left, also called the **pivot**) of a nonzero row is always strictly to the right of the leading coefficient of the row above it.

For instance, the following matrix is in row echelon form

$$\begin{bmatrix} \mathbf{1} & 2 & -1 & 5 & -4 \\ 0 & 0 & \mathbf{2} & 0 & 5 \\ 0 & 0 & 0 & \mathbf{1} & 3 \end{bmatrix}$$

A **row reduction** is a process of reducing a given matrix to a row echelon form.

Definition 3.2 (Elementary row operations)**.**

- **Row addition**: a row can be replaced by the sum of that row and a (integer!)multiple of another row.
- **Row switching**: switch two rows.
- **Row inversion**: multiply a row by -1.

We use elementary row operations to reduce the matrix to a row echelon form. For instance, for

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 2 & 1 \\ 3 & 4 & -2 \end{bmatrix}$$

- Add row #1 multiplied by -2 to row #2 to get

$$\begin{bmatrix} 1 & 0 & -1 \\ 0 & 2 & 3 \\ 3 & 4 & -2 \end{bmatrix}$$

- Add row #1 multiplied by -3 to row #3 to get

$$\begin{bmatrix} 1 & 0 & -1 \\ 0 & 2 & 3 \\ 0 & 4 & 1 \end{bmatrix}$$

- Add row #2 multiplied by -2 to row #3 to get

$$\begin{bmatrix} 1 & 0 & -1 \\ 0 & 2 & 3 \\ 0 & 0 & 5 \end{bmatrix}$$

Exercise 3.6. [+5pts] Compute a row echelon form of the matrix

$$\begin{bmatrix} 2 & 0 & -1 \\ 2 & 2 & 1 \\ 3 & 4 & -2 \end{bmatrix}$$

Solution:

- Add row #1 multiplied by -1 to row #3 to get

$$\begin{bmatrix} 2 & 0 & -1 \\ 2 & 2 & 1 \\ 1 & 4 & -1 \end{bmatrix}$$

- Switch row #1 ad #3 to get

$$\begin{bmatrix} 1 & 4 & -1 \\ 2 & 0 & -1 \\ 2 & 2 & 1 \end{bmatrix}$$

- Add row #1 multiplied by -2 to row #2 to get
$$\begin{bmatrix} 1 & 4 & -1 \\ 0 & -8 & 1 \\ 2 & 2 & 1 \end{bmatrix}$$
- Add row #1 multiplied by -2 to row #3 to get
$$\begin{bmatrix} 1 & 4 & -1 \\ 0 & -8 & 1 \\ 0 & -6 & 3 \end{bmatrix}$$
- Add row #3 multiplied by -1 to row #2 to get
$$\begin{bmatrix} 1 & 4 & -1 \\ 0 & -2 & -2 \\ 0 & -6 & 3 \end{bmatrix}$$
- Add row #2 multiplied by -3 to row #3 to get
$$\begin{bmatrix} 1 & 4 & -1 \\ 0 & -2 & -2 \\ 0 & 0 & 9 \end{bmatrix}$$
- Finally, we can multiply row #2 by -1 to get a positive pivot
$$\begin{bmatrix} 1 & 4 & -1 \\ 0 & 2 & 2 \\ 0 & 0 & 9 \end{bmatrix}$$

$\square$