Name: Rajat Rajesh shetty
CWID: 10477484

Assignment-3

Exercise 3.1

S.T. $n = 1105$ is a carmichael number.

$\boxed{1105 = 5 \cdot 13 \cdot 17}$

=) we know that

$\boxed{a^{n-1} \equiv_n 1}$ for every $a \in \mathbb{Z}$

so we need to prove $a^{1104} \equiv_{1105} 1$.

since we have to show a is relatively prime to 1105, $a^{1104} \equiv 1 \bmod 1105$

By using the concept of chinese remainder theorem, we know that

$a^{1104} \equiv 1 \bmod 5$

$a^{1104} \equiv 1 \bmod 13$

$a^{1104} \equiv 1 \bmod 17$.

By fermat's little theorem,

$\boxed{a^{p-1} \equiv 1 \bmod p}$ is relatively prime to p.

By assumption, a is relatively prime to 1105,

$\therefore$ it is relatively prime to 5, 3, 17 as well.

Thus,

$a^{4} \equiv 1 \bmod 5$

$a^{12} \equiv 1 \bmod 13$

$a^{16} \equiv 1 \bmod 17$.

in general,

& thus $\left.\begin{array}{l} a^{4n} \equiv 1 \bmod 5 \\ a^{12n} \equiv 1 \bmod 13 \\ a^{16n} \equiv 1 \bmod 17 \end{array}\right\}$ for any n.

since 4, 12, 16 divides 1104 evenly,

it follows $a^{1104} \equiv 1 \bmod 5$

$a^{1104} \equiv 1 \bmod 13$

$a^{1104} \equiv 1 \bmod 17$.

$\boxed{\therefore a^{1104} \equiv 1 \bmod (1105) \text{ for any } a \in \mathbb{Z}}$

so, we can conclude that 1105 is a carmichael number

Exercise 3.2

Use base 2 Miller - Rabin primality test to show that $N = 341$ is composite.

$\Rightarrow$ So the Miller Rabin primality test tells us

① to generate a random 'a' s.t. $1 < a < n$. satisfying $\gcd(a,n) = 1$.

In our case $a = 2$. ✓

so $\gcd(2, 341) = 1$

② compute q & k s.t. $n-1 = 2^k q$.

$= 2^2 . 85$. ✓

$n - 1 = 340$

$= 2^2 . 85$.

$\therefore 340 = 2^2 . 85$.

~~for~~ we know that for modulo 341,

$2^{85} \equiv 32 \not\equiv 1$

& $2^{170} \equiv 1 \not\equiv -1$

~~(Hence 341 fails the test for base 2)~~

because

$$\boxed{\begin{aligned} 2^{85} &\equiv_{341} 32 \\ 2^{170} &\equiv_{341} 32^2 \\ 2^{170} &\equiv_{341} 1 \end{aligned}}$$

341 is composite & we get

$2^{340} \equiv (2^{170})^2 \equiv 1 \mod 341$.

$\therefore$ we can conclude that 341 is a pseudo prime to base 2.

or

① perform $n-1$ s.t. $n-1 = m \times 2^k$

② if $k \leq 1$ calculate $T = a^m \mod n$

if $(T = \pm 1)$ no is composite

③ if $k > 1$, calculate $T = T^2 \mod n$

if $(T = 1)$ no is composite

if $(T = -1)$, no is prime.

else, no is composite

$n = 341$ $a = 2$

$n - 1 = m \times 2^k$ where $k = 2$.

$= 2^2 . 85$.

$T = 2^{85} \mod 341$

$= 2^{32} . 2^{32} . 2^{16} . 2^4 . 2^1 \mod 341$

$= (4 . 4 . 64 . 16 . 2) \mod 341$

$= 32$ //

Since $k > 1$,

$T = 32^2 \mod 341$

$= 1024 \mod 341$

$\Rightarrow \underline{1}$

$\therefore$ n is composite following the algorithm //

Exercise 3.3

for $N=6994241$ use pollard's p-1 algorithm with $a=2$ to find non trivial factor.

⇒ The Pollard's p-1 algorithm tells you to pick random a st $\gcd(a,N)=1$.

& we need to calculate $\boxed{d=\gcd(N, a^{n!}-1)}$

⇓ using formula

Iteration(i)

$B=1 \quad 2^{1!}=2 \quad \gcd(2-1, 6994241)=1$

$B=2 \quad 2^{2!}=4 \quad \gcd(4-1, 6994241)=1$

$B=3 \quad 2^{3!}=(2^{2!})^3=(4)^3 \quad \gcd(64-1, 6994241)=1$

$B=4 \quad 2^{4!}=(2^{3!})^4=2788734 \quad \gcd(2788734-1, 6994241)=1$

$\gcd(2788733, 6994241)=1$

$64^4 \bmod 6994241$

$\Rightarrow 2788734$

$B=5 \quad 2^{5!}=(2^{4!})^5=(2788734)^5 \bmod 6994241$

$=3834705 \quad \gcd(3834705-1, 6994241)$

$\gcd(3834704, 6994241)$

$=1$

$B=6 \quad 2^{6!}=(2^{5!})^6=(3834705)^6 \bmod 6994241 \quad \gcd(513770-1, 6994241)$

$\Rightarrow 513770 \quad \Rightarrow 1$

$B=7 \quad 2^{7!}=(2^{6!})^7=443653 \quad \gcd(443653-1, 6994241)$

$513770^7 \bmod 6994241 \Rightarrow \gcd(443652, 6994241)$

$\Rightarrow 3361$

so, on the 7th iteration we get prime factor 3361 of n. $\boxed{\therefore N=\underset{p}{3361} \times \underset{q}{2081}}$

PPF

$(p-1)\ 3360=2^5\times3\times7\times5 \quad (q-1)\ 2080=2^5\times5\times13$

gcd(1, 6994241)
=1

gcd(63, 6994241)
=1

gcd(3, 6994241)
=1

Exercise 3.4

Let $N = 377753$. Given the relations

$$620^2 \equiv_N 6647 = 17^2 \cdot 23,$$
$$621^2 \equiv_N 7888 = 2^4 \cdot 17 \cdot 29,$$
$$645^2 \equiv_N 38272 = 2^7 \cdot 13 \cdot 23,$$
$$655^2 \equiv_N 51272 = 2^3 \cdot 13 \cdot 17 \cdot 29,$$

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

$\Rightarrow$ we have to find a & b:

we know that for factorization of N through difference, we have,

reason
$(2^7 \cdot 13 \cdot 17^2 \cdot 23 \cdot 29)$
$- (849 \times 377753)$
$\Rightarrow 45335$

$$a^2 \equiv_N b^2$$

$$\Rightarrow (a-b)(a+b) \Rightarrow a^2 - b^2 = Nq \text{ for some } q \in \mathbb{Z}$$

$$(620 \cdot 621 \cdot 645 \cdot 655 \pmod N)^2 \equiv (2^7 \, 13 \cdot 17^2 \cdot 23 \cdot 29)^2 \pmod N$$

reason
$(620 \times 621 \times 645 \times 655 - 1377753 \times 430602) = (127194)$

$$\Rightarrow (127194^2 = 45335^2 \pmod N) \quad \boxed{127194^2 \equiv_N 45335^2}$$

or $\boxed{127194^2 \equiv_{377753} 45335^2}$

Check
$= 751 \cdot 503$
$= 377753$

$\therefore \boxed{a = 127194}$ & $\boxed{b = 45335}$

$\therefore \gcd(a-b, N) \Rightarrow \gcd(127194 - 45335, 377753)$

$\Rightarrow 751$ which is a factor in N.

Exercise 3.5

For $N = 1111$, $f(x) = x^2 + 1$ & $x_1 = 5$ run four iterations (compute four gcds) of the pollard's rho algorithm & get a non trivial factor of N.

formula
$\boxed{x_i \equiv_p x_{2i}}$

$\Rightarrow$ Given $N = 1111$, $f(x) = x^2 + 1$, & $x_1 = 5$.

$f(x_1) = 5^2 + 1$
$= 26$

$x_1 = 5 = f(x_0)$

1st iteration
$x_2 = 26 = f(x_1)$

$\gcd(x_2 - x_1, n) \Rightarrow \gcd(21, 1111)$

$\gcd(21, 1111)$: $\frac{\cancel{21 \times 1111}}{\cancel{3 \times 7 \times 11} \times 101}$ 21

$\Rightarrow 1$

2nd iteration

$x_3 = 677 = f(x_2)$

reason

$f(x_2) = 26^2 + 1$

$\Rightarrow 676 + 1$

$\Rightarrow \cancel{0676}$

$\Rightarrow \underline{677}$ ✓

$\gcd(651, 1111)$

$= \frac{651 \times 1111}{723261}$

$= \underline{1}$

$$\begin{array}{r|l} 3 & 651, 1111 \\ \hline 11 & 217, 1111 \\ \hline & 217, 101 \end{array}$$

3rd iteration

$x_4 \Rightarrow 598 = f(x_3)$

reason

$f(x_3) = (677)^2 + 1$

$\Rightarrow 458330$
mod 1111

$\Rightarrow 598.$ ✓

$\therefore \gcd(x_4 - x_2, n)$

$\Rightarrow \gcd(598 - 26, 1111)$

$= \boxed{11}$ Non trivial

$\gcd(572, 1111)$

$\Rightarrow \frac{572 \times 1111}{57772}$

$= \underline{11}$

$$\begin{array}{r|l} 2 & 572, 1111 \\ \hline 11 & 286, 1111 \\ \hline 13 & 286, 101 \\ \hline & 2, 101 \end{array}$$

4th iteration

$x_5 \Rightarrow 974 = f(x_4)$

$f(x_4) = (598)^2 + 1$

$= 357605 \bmod 1111$

$\Rightarrow 974.$

~~$\gcd(x_5 - x_4, n) = \gcd(974 - 598, 1111)$~~

$\Rightarrow \cancel{1}$

$\gcd(21, 1111)$

$= \frac{21 \times 1111}{11 \times 7 \times 3 \times 101}$

$= \underline{1}$

$$\begin{array}{r|l} 11 & 21, 1111 \\ \hline 7 & 21, 101 \\ \hline & 3, 101 \end{array}$$

$\therefore$ Non trivial factor of N is 11

Exercise 3.6 compute a row echelon form of the matrix.

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

$\Rightarrow$ steps $\begin{pmatrix} 2 & 0 & -1 \\ 2 & 2 & 1 \\ 3 & 4 & -2 \end{pmatrix}$ swap

① Lets perform : $R_1 \leftrightarrow R_3$

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

② $R_2 \leftarrow R_2 - 2/3 \cdot R_1$

$$= \begin{pmatrix} 3 & 4 & -2 \\ 0 & -2/3 & 7/3 \\ 2 & 0 & -1 \end{pmatrix}$$

because

$2 - \frac{2}{3} \cdot 3 = 0$

$2 - \frac{2}{3} \times 4 = -\frac{2}{3}$

$1 - \frac{2}{3} \times -2 = 7/3$

(3) step $R_3 \leftarrow R_3 - 2/3 \cdot R_1$

$$= \begin{pmatrix} 3 & 4 & -2 \\ 0 & -2/3 & 7/3 \\ 0 & -8/3 & 1/3 \end{pmatrix} \leftarrow$$

$2 - \frac{2}{\cancel{3}} \cdot \cancel{3}$

$\underline{\underline{0}}$

$0 - \frac{2}{3} \times 4$

$\underline{\underline{-8/3}}$

$-1 - \frac{2}{3} \times -2$

$= \underline{\underline{1/3}}$

step (4) Lets swap matrix row : $R_2 \leftrightarrow R_3$.

$$= \begin{pmatrix} 3 & 4 & -2 \\ 0 & -8/3 & 1/3 \\ 0 & -2/3 & 7/3 \end{pmatrix}$$

step 5

(5) $R_3 \leftarrow R_3 - 1/4 \cdot R_2$

row echelon form $\Rightarrow$

$$= \begin{pmatrix} 3 & 4 & -2 \\ 0 & -8/3 & 1/3 \\ 0 & 0 & 9/4 \end{pmatrix}$$

$0 - 1/4 \cdot 0$

$\underline{\underline{0}}$

$-\frac{2}{3} - 1/4 \times -8/3$

$-\frac{2}{3} + \frac{2}{3} = \underline{\underline{0}}$

$7/3 - 1/4 \cdot 1/3$

$= \underline{\underline{9/4}}$