Peter Rauscher **HW 3** MA 503

I pledge my honor that I have abided by the Stevens Honor System.

3.1) $n=1105$ $\quad n=17\cdot 65=17\cdot 13\cdot 5$

$$a^{1104}\equiv_{1105} 1 \iff \begin{cases} a^{1104}\equiv_5 (a^4)^{276}\equiv 1 \\ a^{1104}\equiv_{13} \equiv (a^{12})^{92}\equiv 1 \\ a^{1104}\equiv_{17} 1\equiv (a^{16})^{69}\equiv 1 \end{cases}$$

Using FLT, $a^4\equiv_5 1\equiv (a^4)^{276}$

$a^{12}\equiv_{13} 1\equiv (a^{12})^{92}$

$a^{16}\equiv_{17} 1\equiv (a^{16})^{69}$

So, $a^{1104}\equiv_{(13\cdot 17\cdot 5)} 1$ or $a^{1104}\equiv_{1105} 1$

and thus 1105 is carmichael.

3.2) $N=341$ $\quad a=2$

$N-1=2^k q$

$341-1=2^2\cdot 85$ $\quad q=85$ $\quad K=2$

$2^{85} \bmod 341 = 32 \not\equiv 1$

$2^{2^0 q} \bmod 341 \not\equiv -1$

$2^{2^1 q} \bmod 341 = 1 \not\equiv -1$

The results of the Miller-Rabin primality test cannot prove 341 to be probably prime, therefore it is a composite number

Exercise 3.3) $N = 8611 \quad a = 2$

$2^{1!} \equiv 2 \quad \gcd(2-1, 8611) = 1$
$2^{2!} \equiv 4 \quad \gcd(4-1, 8611) = 1$
$2^{3!} \equiv 64 \quad \gcd(64-1, 8611) = 1$
$2^{4!} \equiv 2988 \quad \gcd(2988-1, 8611) = 1$
$2^{5!} \equiv 7039 \quad \gcd(7039-1, 8611) = 1$
$2^{6!} \equiv 6105 \quad \gcd(6105-1, 8611) = 109$

A nontrivial factor of $N = 8611$ is 109

Exercise 3.4)

$620^2 \equiv 17^2 \cdot 23$ | $621^2 \equiv 2^4 \cdot 17 \cdot 29$

$645^2 \equiv 2^7 \cdot 13 \cdot 23$ | $655^2 \equiv 2^3 \cdot 13 \cdot 17 \cdot 29$

Multiplying these together,
we get

$620^2 \cdot 645^2 \equiv 2^7 \cdot 13 \cdot 17^2 \cdot 23^2$ | $621^2 \cdot 655^2 \equiv 2^7 \cdot 13 \cdot 17^2 \cdot 29^2$

multiply both sides by 29^2 | multiply both sides by 23^2

$620^2 \cdot 645^2 \cdot 29^2 \equiv 2^7 \cdot 13 \cdot 17^2 \cdot 23^2 \cdot 29^2$ | $621^2 \cdot 655^2 \cdot 23^2 \equiv 2^7 \cdot 13 \cdot 17^2 \cdot 23^2 \cdot 29^2$

so,

$$620^2 \cdot 645^2 \cdot 29^2 \equiv_N 621^2 \cdot 655^2 \cdot 23^2$$
$$a^2 \equiv_N b^2$$

so $a = 620 \cdot 645 \cdot 29 = 11597100$ $\quad b = 621 \cdot 655 \cdot 23 = 9355365$

$\gcd(11597100 - 9355365, 377753) = 751$
(using wolfram alpha)

$\boxed{a = 11597100,\ b = 9355365,\ \gcd(a-b, N) = 751}$

Exercise 3.5

$N = 8611$

$x_1 = 2$

$f(x) = x^2 + 1$

$x_1 = 2$

$x_2 = 2^2 + 1 = 5 \quad \gcd(5-2, 8611) = 1$

$x_3 = 5^2 + 1 = 26$

$x_4 = 26^2 + 1 = 677 \quad \gcd(677-5, 8611) = 1$

$x_5 = 677^2 + 1 = 458330 \equiv 1947$

$x_6 = 1947^2 + 1 \equiv 1970 \quad \gcd(1970-26, 8611) = 1$

$x_7 = 1970^2 + 1 \equiv 5951$

$x_8 = 5951^2 + 1 \equiv 5970 \quad \gcd(5970-677, 8611) = 79$

$\boxed{\text{A non-trivial factor of } N \text{ is } 79}$