MATH 470: Communications and Cryptography

Homework 7

Due date: 18 October 2023 *Name: Huy Lai*

Problem 1. Illustrate the quadratic sieve, as was done in Fig. 3.3 (page 161), by sieving prime powers up to B on the values of $F(T) = T^2 - N$ in the indicated range. Sieve $N = 493$ using prime powers up to $B = 11$ on values from $F(23)$ to $F(38)$. Use the relation(s) that you find to factor N.

Solution:
The Quadratic Sieve is as follows

23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
36	83	132	183	236	291	348	407	468	531	596	663	732	803	876	951
$\downarrow 2$		$\downarrow 2$		$\downarrow 2$		$\downarrow 2$		$\downarrow 2$		$\downarrow 2$		$\downarrow 2$		$\downarrow 2$	
18	83	66	183	118	291	174	407	234	531	298	663	366	803	438	951
$\downarrow 3$			$\downarrow 3$			$\downarrow 3$			$\downarrow 3$			$\downarrow 3$			$\downarrow 3$
6	83	66	61	118	291	58	407	234	177	298	663	122	803	438	317
		$\downarrow 3$			$\downarrow 3$			$\downarrow 3$			$\downarrow 3$			$\downarrow 3$	
6	83	22	61	118	97	58	407	78	177	298	221	122	803	146	317
$\downarrow 2^2$		$\downarrow 2^2$		$\downarrow 2^2$		$\downarrow 2^2$		$\downarrow 2^2$		$\downarrow 2^2$		$\downarrow 2^2$		$\downarrow 2^2$	
3	83	11	61	59	97	29	407	39	177	149	221	61	803	73	317
								$\downarrow 3^2$							
3	83	11	61	59	97	29	407	13	177	149	221	61	803	73	317
$\downarrow 3^2$									$\downarrow 3^2$						
1	83	11	61	59	97	29	407	13	59	149	221	61	803	73	317
		$\downarrow 11$											$\downarrow 11$		
1	83	1	61	59	97	29	407	13	59	149	221	61	73	73	317
							$\downarrow 11$								
1	83	1	61	59	97	29	37	13	59	149	221	61	73	73	317

Table 1: Sieving $n = 493$

The two values $F(23)$ and $F(25)$ have been sieved down to 1, yielding the congruences

$$F(23) \equiv 36 \equiv 2^2 \cdot 3^2 \mod 493 \quad \text{and} \quad F(25) \equiv 132 \equiv 2^3 \cdot 3 \cdot 11 \mod 493$$

Since $F(23)$ is itself congruent to a square, we can compute $\gcd(23-2\cdot 3, 493) \equiv 17$ which gives the factorization $493 = 17 \cdot 29$.

Problem 2. Let p be an odd prime and let a be an integer with $p \nmid a$. Prove that $a^{\frac{p-1}{2}} \equiv 1 \mod p$ if and only if a is a quadratic residue modulo p.

Solution:
First we prove that if $a^{\frac{p-1}{2}} \equiv 1 \mod p$, then a is a quadratic residue modulo p.

Proof. Let g be a primitive root modulo p such that $a \equiv g^k \mod p$ for some integer k.

$$a^{\frac{p-1}{2}} \equiv 1 \mod p$$
$$(g^k)^{\frac{p-1}{2}} \equiv 1 \mod p$$

Since g is a primitive root, it has order $p-1$.
By proposition, $p-1 \mid k \cdot \dfrac{p-1}{2}$ which can be rewritten as $p-1 \mid \dfrac{k}{2}(p-1)$.
This requires that $\dfrac{k}{2} \in \mathbb{Z}$

Let $\kappa \equiv g^{\frac{k}{2}} \mod p$

$$\kappa^2 \equiv g^{2\cdot\frac{k}{2}} \mod p$$
$$\kappa^2 \equiv g^k \mod p$$
$$\kappa^2 \equiv a \mod p$$

From this, we have found an integer that satisfies the definition of a quadratic residue. □

Next we prove that if a is a quadratic residue modulo p, then $a^{\frac{p-1}{2}} \equiv 1 \mod p$.

Proof. Since a is a quadratic residue, $\exists c \in \mathbb{Z}$ such that $c^2 \equiv a \mod p$.
Additionally, $p \nmid c$ since $p \mid c$ would imply that $c \equiv 0 \mod p$ and cannot square to $a \not\equiv 0 \mod p$.

$$c^2 \equiv a \mod p$$
$$(c^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \mod p$$
$$c^{p-1} \equiv a^{\frac{p-1}{2}} \mod p$$

From this we can apply Fermat's Little Theorem to c^{p-1} and get that

$$a^{\frac{p-1}{2}} \equiv 1 \mod p$$

□

Problem 3. Let p be a prime satisfying $p \equiv 3 \mod 4$. Let a be a quadratic residue modulo p. Prove that the number

$$b \equiv a^{\frac{p+1}{4}} \pmod{p}$$

has the property that $b^2 \equiv a \pmod{p}$

Solution:
The proof is as follows

Proof.

$$\begin{aligned} b^2 &\equiv a^{\frac{p+1}{2}} \mod p \\ &\equiv a^{1+\frac{p-1}{2}} \mod p \\ &\equiv a \cdot a^{\frac{p-1}{2}} \mod p \end{aligned}$$

Since a is a quadratic residue, we use the proof from question 2 and get that

$$a^{\frac{p-1}{2}} \equiv 1 \mod p$$

Using this fact we get

$$b^2 \equiv a \mod p$$

□

Problem 4. Recall that $p = 9907$ is a prime. Use quadratic reciprocity to compute $\left(\frac{1002}{9907}\right)$.

Solution:
First note that $9907 \equiv 3 \mod 4$ and $9907 \equiv 3 \mod 8$

$$\begin{aligned}
\left(\frac{1002}{9907}\right) &= \left(\frac{2 \cdot 3 \cdot 167}{9907}\right) \\
&= \left(\frac{2}{9907}\right)\left(\frac{3}{9907}\right)\left(\frac{167}{9907}\right) \\
&= -1\left(\frac{3}{9907}\right)\left(\frac{167}{9907}\right) \\
&= -1\left(-\frac{9907}{3}\right)\left(-\frac{9907}{167}\right) \\
&= -\left(-\frac{1}{3}\right)\left(-\frac{54}{167}\right) \\
&= \left(-\frac{54}{167}\right) \\
&= -\left(\frac{2 \cdot 27}{167}\right) \\
&= -\left(\frac{2}{167}\right)\left(\frac{27}{167}\right) \\
&= -\left(\frac{27}{167}\right) \\
&= -\left(\frac{167}{27}\right) \\
&= -\left(\frac{5}{27}\right) \\
&= -\left(\frac{27}{5}\right) \\
&= -\left(\frac{2}{5}\right) \\
&= -1
\end{aligned}$$

Problem 5. Let p be an odd prime. Prove that the number of quadratic residues modulo p is exactly $\dfrac{p+1}{2}$

Solution:
The integer 0 is a trivial example of a quadratic residue so $+1$ will be added to the final number count.

Proof. The quadratic residues of p are the integers which will result from the evaluation of the squares:

$$1^2, 2^2, 3^2, \cdots, (p-1)^2 \mod p$$

and so these $p-1$ integers fall into congruent pairs modulo p, namely:

$$\begin{aligned} 1^2 &\equiv (p-1)^2 \mod p \\ 2^2 &\equiv (p-2)^2 \mod p \\ &\vdots \\ \left(\frac{p-1}{2}\right)^2 &\equiv \left(\frac{p+1}{2}\right)^2 \mod p \end{aligned}$$

Therefore, each quadratic residue modulo p is congruent modulo p to one of the $\dfrac{p-1}{2}$ integers:

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

All we need to do now is show that no two of these integers are congruent modulo p.
Suppose that $r^2 \equiv s^2 \mod p$ for some $1 \leq r \leq s \leq \dfrac{p-1}{2}$.
What we need to do is prove that $r = s$.

By proposition, $p \mid (r-s)(r+s)$.
This means that either $p \mid (r-s)$ or $p \mid (r+s)$
$p \nmid (r+s)$ as $2 \leq r+s \leq p-1$.

This leaves $p \mid (r-s)$
As $0 \leq r-s < \dfrac{p-1}{2}$, this condition can only happen when $r-s=0$ or equivalently, when $r=s$.

Therefore, there must be exactly $\dfrac{p-1}{2} + 1 = \dfrac{p+1}{2}$ quadratic residues modulo p. □

Problem 6. My RSA public key is (N, e), where

$$N = 342647387528779375670375098162296213741958911642475645613557064143782 7$$
$$e = 65537$$

I receive the following ciphertext:

$$c = 240055613222981848930564951534665484829848347733461966659128028412676 9$$

Implement the quadratic sieve to factor N and decrypt the message.

Solution:
Who knows bro.