Exam #3 Review Question Solutions

1) What is the prime factorization of 175?

$175 = 5^2 \times 7$

2) Prove that 2 is a generator mod 13.

$$\begin{align*}
2^1 &\equiv 2 \mod 13 \\
2^2 &\equiv 4 \mod 13 \\
2^3 &\equiv 8 \mod 13 \\
2^4 &\equiv 3 \mod 13 \\
2^5 &\equiv 6 \mod 13 \\
2^6 &\equiv 12 \mod 13 \\
2^7 &\equiv 11 \mod 13 \\
2^8 &\equiv 9 \mod 13 \\
2^9 &\equiv 5 \mod 13 \\
2^{10} &\equiv 10 \mod 13 \\
2^{11} &\equiv 7 \mod 13 \\
2^{12} &\equiv 1 \mod 13
\end{align*}$$

This shows that the smallest positive integer for which $2^k \equiv 1 \mod 13$ is 12, this 2 is a generator.

3) What is the remainder when $37^{129}$ is divided by 80?

$$\phi(80) = \phi((5)(16)) = \phi(5) \phi(16) = (5 - 1)(16 - 8) = 32.$$ (4 pts)

Thus, $37^{32} \equiv 1 \mod 80$.

$$37^{129} \equiv (37^{32})^4(37) \mod 80$$ (3 pts)

$$\equiv 1^4(37) \mod 80$$

$$\equiv 37 \mod 80$$ (1 pt)

4) In an RSA scheme, $p = 7$, $q = 13$ and $e = 5$. What is $d$?

$$n = 7 \times 13 = 91$$

$$\phi(n) = (7 - 1)(13 - 1) = 72.$$ (3 pts)

$$ed \equiv 1 \mod 72$$

$$5d \equiv 1 \mod 72$$

Thus, we must find $5^{-1} \mod 72$. Use the Extended Euclidean Algorithm:

$$72 = 14 \times 5 + 2$$

$$5 = 2 \times 2 + 1$$ (3 pts)

$$5 - 2 \times 2 = 1$$

$$5 - 2(72 - 14 \times 5) = 1$$

$$5 - 2 \times 72 + 28 \times 5 = 1$$

$$29 \times 5 - 2 \times 72 = 1$$ (3 pts)
Consider the equation mod 72 and we get:

\[29 \times 5 \equiv 1 \mod 72.\]

It follows that \(d = 29\). (1 pt)

5) Factor 20701 using the Fermat Factoring method.

\[\sqrt{20701} \approx 143.9, \text{ so}\]

\[144^2 - 20701 = 35 \text{ (not a perfect square) (3 pts)}\]

\[145^2 - 20701 = 324 = 18^2. \quad (3 \text{ pts})\]

It follows that:

\[145^2 - 18^2 = 20701 \quad (1 \text{ pt})\]

\[(145 - 18)(145 + 18) = 20701\]

Thus, 20701 factored is 127 x 163. (1 pt)

6) Given that \(n = 391\), what is \(\phi(n)\)?

\[391 = 23 \times 17, \phi(391) = (23-1)(17-1) = 22 \times 16 = 352\]

7) What is the value of \(197^{422} \mod 211\)?

Using Fermat's theorem, we have that \(197^{210} = 1 \mod 211\), since 211 is prime. It follows that

\[197^{422} = (197^{210})^2(197)(197) \mod 211\]

\[= 1^2(-14)(-14) \mod 211\]

\[= 196 \mod 211\]

8) In an RSA system, \(n = 391\) and \(e = 137\), what is \(d\)?

We need to solve for \(d\) in the equation 137d = 1 mod 352.

So, we must run the Extended Euclidean Algorithm:

\[352 = 2 \times 137 + 78\]

\[137 = 1 \times 78 + 59\]

\[78 = 1 \times 59 + 19\]

\[59 = 3 \times 19 + 2\]

\[19 = 9 \times 2 + 1\]
2 = 2x1

Now, we have:

\[ 19 - 9x2 = 1 \]
\[ 19 - 9x(59 - 3x19) = 1 \]
\[ 19 - 9x59 + 27x19 = 1 \]
\[ 28x19 - 9x59 = 1 \]
\[ 28x(78 - 59) - 9x59 = 1 \]
\[ 28x78 - 28x59 - 9x59 = 1 \]
\[ 28x78 - 37x59 = 1 \]
\[ 28x78 - 37x(137 - 78) = 1 \]
\[ 28x78 - 37x137 + 37x78 = 1 \]
\[ 65x78 - 37x137 = 1 \]
\[ 65x(352 - 2x137) - 37x137 = 1 \]
\[ 65x352 - 130x137 - 37x137 = 1 \]
\[ 65x352 - 167x137 = 1 \]

Thus \( d = -167 = (352 - 167) = 185 \mod 352. \)

\( d = 185 \)

9) In a Diffie-Hellman Key Exchange, Alice and Bob agree upon the public keys \( p = 17 \) and \( g = 3 \). Alice picks the secret key \( a = 4 \) and Bob picks the secret key \( b = 7 \). What value does Alice send Bob? What value does Bob send Alice? What is their shared secret key?

Alice sends Bob \( 3^4 \mod 17 = 81 \mod 17 = 13. \)
Bob sends Alice \( 3^7 \mod 17 = (27)(27)(3) \mod 17 = (10)(10)(3) \mod 17 = 11. \)

Their shared key (calculated by Alice) is \( 11^4 \mod 17 = (121)(121) \mod 17 = 4 \mod 17, \) since \( 121 = 2 \mod 17. \)

10) In practice, why is the Miller-Rabin algorithm used for primality testing, instead of the AKS algorithm, even though the latter is always correct while the former isn’t?

The probability that Miller-Rabin is incorrect once it’s iterated a reasonable number of times is extremely low (less than \( 1 \) in \( 10^{20} \) is quite easy to achieve). In addition, Miller-Rabin is much quicker than AKS in practice. Both facts in combination are why Miller-Rabin is preferable.
11) Consider the Elliptic Curve $E_{29}(3, 11)$. Let $p$ be the point $(8, 5)$ on this curve and $q$ be the point $(20, 26)$ on this curve. Determine $P + Q$.

$$
\lambda = \frac{y_q - y_p}{x_q - x_p} = \frac{26 - 5}{20 - 8} \mod 29 = 21 \times 12^{-1} \mod 29
$$

We must find $12^{-1} \mod 29$:

$$
29 = 2 \times 12 + 5 \\
12 = 2 \times 5 + 2 \\
5 = 2 \times 2 + 1 \\
5 - 2 \times 2 = 1 \\
5 - 2(12 - 2x5) = 1 \\
5 \times 5 - 2 \times 12 = 1 \\
5(29 - 2x12) - 2x12 = 1 \\
5 \times 29 - 12 \times 12 = 1 \\
12^{-1} \equiv -12 \equiv 17 \mod 29
$$

Thus, $\lambda = 21 \times 12^{-1} \equiv 21 \times 17 \equiv 357 \equiv 9 \mod 29$.

$$
x = \lambda^2 - x_p - x_q \equiv 9^2 - 8 - 20 \equiv 53 \equiv 24 \mod 29 \\
y = (\lambda(x_p - x) - y_p) \equiv (9(8 - 24) - 5) \equiv (9 \times 13 - 5) \equiv 112 \equiv 25 \mod 29
$$

Thus, the desired sum is the point $(24, 25)$.

12) Consider the Elliptic Curve $E_{29}(3, 11)$. Let $P$ be the point $(8, 5)$ on this curve. Determine $2P$.

$$
\lambda = \frac{3x_p^2 + a}{2y_p} = \frac{3(8)^2 + 3}{2(5)} = \frac{195}{10} \equiv \frac{21}{10} \mod 29 = 21 \times 10^{-1} \mod 29
$$

To save some work, we can eyeball that $10^{-1} \equiv 3 \mod 29$, since $3 \times 10 = 30$ and $30 \equiv 1 \mod 29$.

Thus, we have $\lambda = 21 \times 3 \equiv 63 \equiv 5 \mod 29$

Now, we can solve for $x$ and $y$:

$$
x = \lambda^2 - 2x_p \equiv 5^2 - 2(8) \equiv 9 \mod 29 \\
y = (\lambda(x_p - x) - y_p) \equiv (5(8 - 9) - 5) \equiv -10 \equiv 19 \mod 29
$$

Thus, the desired sum is the point $(9, 19)$. 