Number Theory and Cryptography
Practice Midterm 1 (with solutions)

Choose six problems from the list below; each problem is worth 16 points. Please show all work; for true/false problems, give a proof or a counterexample.

1. **True or False:** If a, b are nonzero integers such that $a|bc$ and $a \nmid c$, then $a|b$.
Solution: False. $a = 4$, $b = 2$, $c = 6$ is a counterexample.

2. **True or False:** For any integer n, the product $n(n+1)(n+2)$ is a multiple of 6.
Solution: True. This number is always even, since one of n or $n+1$ is always even. Mod 3, we have $n(n+1)(n+2) = 0 \cdot 1 \cdot 2 = 0$, or $1 \cdot 2 \cdot 0 = 0$, or $2 \cdot 0 \cdot 1 = 0$, according to the value of $n \bmod 3$, so $n(n+1)(n+2)$ is always divisible by 3. Since 2 and 3 both appear in the prime factorization of $n(n+1)(n+2)$, this number is a multiple of six.

3. Prove that 5 is a generator of $\mathbf{Z}_{47}^{\times}$. Prove that $5^{18} = 2 \bmod 47$, and use this to find $\sqrt{2}$ in $\mathbf{Z}_{47}$.
Solution: Since $\varphi(47) = 46 = 2 \cdot 23$, we need to check that $5^2 \neq 1 \bmod 47$ and $5^{23} \neq 1 \bmod 47$. Clearly $5^2 = 25$. Now mod 47, we calculate

$$\begin{aligned}
5^{23} &= 5^3 \cdot (5^4)^5 \\
&= 125 \cdot (125 \cdot 5)^5 \\
&= 31 \cdot (31 \cdot 5)^5 \\
&= 31 \cdot (14)^5 \\
&= 31 \cdot (196)^2 \cdot 14 \\
&= 31 \cdot (8)^2 \cdot 14 \\
&= 31 \cdot 64 \cdot 14 \\
&= 31 \cdot 17 \cdot 14 \\
&= 31 \cdot (196 + 42) \\
&= 31 \cdot (4 \cdot 47 + 50) \\
&= 31 \cdot 3 \\
&= 93 \\
&= -1.
\end{aligned}$$

Therefore 5 is a generator. Next, note (by what we already did) that $5^4 = 14$ and $5^8 = 8$, so $5^{18} = 5^{8+8} \cdot 25 = 64 \cdot 25 = 17 \cdot 25 = 425 = 9 \cdot 43 + 2 = 2$. Therefore, since $2 = 5^{18} = (5^9)^2$, we have $\sqrt{2} = 5^9 = 5^8 \cdot 5 = 8 \cdot 5 = 40$.

4. State and prove Euclid's lemma.
Solution:
Statement: If a, b are nonzero integers and p is a prime such that $p|ab$, then $p|a$

and/or $p|b$.
Proof: It suffices to prove that if $p|ab$ and $p \nmid a$, then $p|b$. Since $p \nmid a$, we have $(a,p) = 1$, so we can write $1 = ma + np$ for some integers m, n by Bezout's lemma. Multiplying by p gives

$$\begin{aligned} b &= (ma + np)b \\ &= mab + npb \\ &= (mq + nb)p \end{aligned}$$

where q is the integer with $ab = qp$, so p divides b.

5. **True or False:** If $n = 1 \pmod 4$, then n can be written as $n = x^2 + y^2$ for some integers x, y.
Solution: False: 21 is a counterexample, since $21 - 1 = 20$, $21 - 4 = 17$, $21 - 9 = 12$, and $21 - 16 = 5$, and none of the right-hand sides here are squares. 33 is also a counterexample.

6. Find two roots of the equation $x^2 + x - 1 = 0 \pmod{19}$. Show that this polynomial has no other roots in $\mathbf{Z}_{19}$.
Solution: Brute-force listing of all the values mod 19 of this polynomial for $x = 0, 1, 2, ..., 18$ shows that 4 and $14 = -5$ are the only roots.
A slightly better solution: Since this polynomial has degree two, we know it can have at most two roots in $\mathbf{Z}_p$. Starting at $x = 0, 1, 2, etc.$ we tabulate the values and find quickly that 4 is a root. Then we try factoring the polynomial as $x^2 + x - 1 = (x - 4)(x - r)$ where r is another root we haven't found yet. Expanding the right-hand side gives $x^2 - (4 + r)x + 4r$, so comparing the coefficients of x we must have $4 + r = -1 = 18$, so $r = 18 - 4 = 14$, and one checks that this is indeed a root.

7. Prove that if p is an odd prime which can be written as $p = x^2 + 2y^2$ for some integers x, y, then $p = 1 \text{ or } 3 \bmod 8$. Give examples of primes of either type.
Solution: First we find the squares in $\mathbf{Z}_8$; this is easy; we have

$$\begin{aligned} 0^2 &= 0 \\ 1^2 &= 1 \\ 2^2 &= 4 \\ 3^2 &= 1 \\ 4^2 &= 0 \\ 5^2 &= 1 \\ 6^2 &= 4 \\ 7^2 &= 1, \end{aligned}$$

so the squares in $\mathbf{Z}_8$ are $\{0, 1, 4\}$. Hence, the values of the expression $x^2 + 2y^2$ in $\mathbf{Z}_8$ are the elements $A + B \in \mathbf{Z}_8$ where $A \in \{0, 1, 4\}$ is a square and $B \in \{0, 2\}$

is twice a square. The values of $A + B$ of this type are exactly $\{0, 1, 2, 3, 4, 6\}$. But if $p = x^2 + 2y^2$ is an odd prime, then $p \neq 0, 2, 4, 6 \bmod 8$, and therefore $p = 1$ or $3 \bmod 8$. $17 = 3^2 + 2 \cdot 2^2$ is an example which is $1 \bmod 8$. $43 = 3^2 + 2 \cdot 4^2$ is an example which is $3 \bmod 8$.

8. Prove that if $p > 2$ is prime and $u \in \mathbf{Z}_p^\times$ is a generator, then $\sqrt{u}$ doesn't exist in $\mathbf{Z}_p$.
Solution: Suppose $\sqrt{u}$ exists, so we have some $x \in \mathbf{Z}_p^\times$ with $x^2 = u$. Since u is a generator, we can write $x = u^n$ for some $n \geq 1$. Squaring both sides gives $u = x^2 = u^{2n}$, so $u^{2n-1} = 1$. This implies $\mathrm{ord}_p(u) | (2n-1)$, but $\mathrm{ord}_p(u) = p - 1$ by assumption, so we get $(p-1) | (2n-1)$. This is a contradiction, since $p - 1$ is even and $2n - 1$ is odd. Therefore $\sqrt{u}$ doesn't exist.

9. Prove that if p is an odd prime such that -1 is a square in $\mathbf{Z}_p$, then $p = 1 \bmod 4$.
Solution: If -1 is a square in $\mathbf{Z}_p$, then we can find some element $x \in \mathbf{Z}_p^\times$ with $x^2 = -1$. Note that $x^4 = (x^2)^2 = (-1)^2 = 1$. Since $x \neq 1$ and $x^2 = -1 \neq 1$ (because $-1 \neq 1$ in $\mathbf{Z}_p$ on account of our assumption that $p > 2$), we see that x has order exactly 4. But the order of any element of $\mathbf{Z}_p^\times$ $p - 1$, so $4 | (p-1)$, i.e. $p = 1 \bmod 4$.

Extra credit: (Omitted.)