Number Theory and Cryptography
Practice Midterm 2 (3/31)

Choose seven problems from the list below; each problem is worth 14 points. Please show all work; for true/false problems, give a proof or a counterexample. As usual, p denotes a prime.

1. **True or False:** 6 is a square in $\mathbf{Z}_{73}$.
Solution. We want to use Euler's criterion, so we need to calculate 6^{36} mod 73. We observe that $6^3 = 216 = 219 - 3 = -3$, so then $6^6 = 9$, $6^{12} = 81 = 8$, and then $6^{36} = (6^{12})^3 = 8^3 = 64 \cdot 8 = -9 \cdot 8 = -72 = 1$. So this is **true:** 6 is a square mod 73.
Alternately, we could use quadratic reciprocity as follows:

$$\begin{aligned}\left(\frac{6}{73}\right) &= \left(\frac{2}{73}\right)\left(\frac{3}{73}\right) \\ &= \left(\frac{3}{73}\right) \\ &= \left(\frac{73}{3}\right) \\ &= \left(\frac{1}{3}\right) \\ &= 1.\end{aligned}$$

2. **True or False:** $x^3 - 1$ has three roots in $\mathbf{Z}_{11}$.
Solution. **False**. $x = 1$ is a root, and any other root would have order exactly 3 - but there aren't any elements in $\mathbf{Z}_{11}$ of order 3, because 3 doesn't divide $\varphi(11) = 10$.

3. **True or False:** There are always $\frac{1}{2}\varphi(n)$ distinct squares in $\mathbf{Z}_n^\times$.
Solution. **False.** If $n = 8$, then $\frac{1}{2}\varphi(8) = 2$, but 1 is the only square in $\mathbf{Z}_8^\times$.

4. Prove that $(p-1)! = -1 \pmod p$. (Hint: Factor the polynomial $x^{p-1} - 1$ mod p and then look at constant terms.)
Solution. By Fermat's little theorem, every element of $\mathbf{Z}_p^\times$ is a root of this polynomial, and the degree of this polynomial equals the size of $\mathbf{Z}_p^\times$, so we can factor the polynomial completely in $\mathbf{Z}_p[x]$ as

$$x^{p-1} - 1 = (x-1)(x-2)(x-3)\cdots(x-p+1).$$

Comparing constant terms, the constant term on the left is -1. The constant term on the right is

$$\begin{aligned}-1 \cdot -2 \cdot -3 \cdot \cdots \cdot -(p-1) &= (-1)^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-1) \\ &= (p-1)!,\end{aligned}$$

so we're done.

5. Prove that if neither 2 nor -1 is a square in $\mathbf{Z}_p$, then $p = 3 \pmod 8$.

Solution. We should look at p mod 8, since the conditions of squareness for -1 and 2 are conditions on p mod 4 and mod 8, respectively. If -1 is not a square mod p, then $p = 3 \bmod 4$, which is the same as $p = 3 \text{ or } 7 \bmod 8$. We also proved that if 2 is not a square mod p, then $p = 3 \text{ or } 5 \bmod 8$. The overlap between the conditions "p is 3 or 7 mod 8" and "p is 3 or 5 mod 8" is exactly "p is 3 mod 8".

6. Prove that there are $\frac{p-1}{2}$ squares in $\mathbf{Z}_p^\times$.
Solution. Suppose a is any square in $\mathbf{Z}_p^\times$, so $a = n^2 \bmod p$ for some $n \in \mathbf{Z}$. Replacing n with n mod p, we can assume that $0 < n < p$, so the map

$$\begin{aligned} T = \{0 < n < p\} &\to \{\text{squares in } \mathbf{Z}_p^\times\} \\ n &\mapsto n^2 \bmod p \end{aligned}$$

hits every square in $\mathbf{Z}_p^\times$. Now suppose two elements $n, m \in T$ go to the same square under this map - this is equivalent to $n^2 = m^2 \bmod p$, which is the same as $p|(n^2 - m^2)$ - and then by Euclid's lemma, this is the same as "$p|(n-m)$ or $p|(n+m)$". If $p|(n-m)$, then since $|n-m| < p$ this forces $n - m = 0$, so $n = m$. If $p|(n+m)$, then since $0 < n + m < p + p = 2p$ by assumption, we must have $n + m = p$. So two distinct guys $n, m \in T$ go to the same square exactly when $n = p - m$. Therefore this map is "2-to-1" - it hits every square exactly twice - so we get $\#T = 2 \cdot \#\{\text{squares in } \mathbf{Z}_p^\times\}$. Since $\#T = p - 1$, this finishes the proof.

7. State and prove Euler's criterion.
Solution.
Euler's criterion: Given any prime p and any integer a with $p \nmid a$, then a is a square in $\mathbf{Z}_p^\times$ if and only if $a^{\frac{p-1}{2}} = 1 \bmod p$.
Proof. Lets look at the polynomial $f = x^{\frac{p-1}{2}} - 1$ mod p. If a is a square mod p, then $a = n^2 \bmod p$, so

$$a^{\frac{p-1}{2}} - 1 = (n^2)^{\frac{p-1}{2}} - 1 = n^{p-1} - 1 = 1 - 1 = 0 \bmod p$$

(using Fermat's little theorem), so every square in $\mathbf{Z}_p^\times$ is a root of f. The degree of f is $\frac{p-1}{2}$, so it can't have more than $\frac{p-1}{2}$ roots mod p; but each square is a root, and by the previous problem there are exactly $\frac{p-1}{2}$ squares, which matches this bound, so the roots of f are exactly the squares mod p.

8. Prove that for any odd integer $n \geq 1$, any prime divisor q of $2^n - 1$ satisfies $q = \pm 1 \pmod 8$.
Solution. Let $q|(2^n - 1)$ be an odd prime as in the problem. Looking mod q, this means that $2^n = 1 \bmod q$. Multiplying both sides by 2, we get $2^{n+1} = 2 \bmod q$. Since $n + 1$ is even, we can write

$$2 = 2^{n+1} = (2^{\frac{n+1}{2}})^2 \bmod q,$$

and therefore 2 is a square mod q. But we proved in class that 2 is a square mod q exactly when $q = \pm 1 \bmod 8$.

9. For which primes $p > 3$ is 3 a square mod p?
Solution sketch. We know that

$$\left(\tfrac{3}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{-3}{p}\right),$$

and we also know that

$$\left(\tfrac{-1}{p}\right) = 1 \Leftrightarrow p = 1 \bmod 4$$

and

$$\left(\tfrac{-3}{p}\right) = 1 \Leftrightarrow p = 1 \bmod 3.$$

Examining various cases, we deduce that

$$\left(\tfrac{3}{p}\right) = 1 \Leftrightarrow p = \pm 1 \bmod 12$$