1 Introduction and Review

2 Wilson's Theorem and Consequences

3 Euler's Criterion for Squares (mod p)

Theorem 8.5 (Euler's Criterion for Squares (mod p)) *Let p be an odd prime number, and let a be an integer coprime to p. Then,*

- *a is square* (mod p)*, if and only if* $a^{(p-1)/2} \equiv 1 \pmod{p}$.
- *a is nonsquare* (mod p)*, if and only if* $a^{(p-1)/2} \equiv -1 \pmod{p}$.

4 Applications of Euler's Criterion

Theorem 8.7 (Fermat's Christmas Theorem) *Let p be a prime number with $p \equiv 1 \pmod{4}$. Then the Diophantine equation $x^2 + y^2 = p$ has a solution. In other words, p can be expressed as the sum of two squares.*

Proposition 8.8 (Minkowski's theorem in the plane) *Consider a grid of parallelograms in the plane, with the origin at a grid point, and a circle centered at the origin. If the area of the circle is greater than 4 times the area of the parallelogram, then the circle contains a grid-point besides the origin.*