ICM 1998, Berlin, Aug. 18–27

Abstracts of Short Communications and Posters

Section:

3. Number Theory and Arithmetic Algebraic Geometry

1991 MS Classification: 11

Clarke, Francis, University of Wales Swansea, UK

Closed Formulas for representing primes by binary quadratic forms

It is a result due to Gauss that if $p = 4k + 1$ is prime and $p = x^2 + y^2$, where x and y are integers and x is odd, with the sign determined by $x \equiv 1 \mod 4$, then

$$x \equiv \frac{1}{2}\binom{2k}{k} \mod p.$$

We discuss various generalisations. For example if p is prime and $4p = x^2 + 19y^2$, where the sign of x is chosen so that x is a quadratic residue modulo 19, then

$$x \equiv (-1)^{(p+1)/2} \sum_{4a+6b=p-1} \binom{2a+2b}{a+b}\binom{a+b}{a} 2^{3a+2b} 19^{a+2b} \mod p.$$