12a

По малой теореме Ферма ap-11(p)

Тогда (a(p-1)/2-1)(a(p-1)/2+1)$ ≡$1(p) => либо a(p-1)/21(p) (1), либо a(p-1)/2-1(p) (2).

Если a – вычет, то x: x2a(p). Тогда a(p-1)/2xp-11(p) (по малой теореме Ферма), => все вычеты являются решениями сравнения (1), а так как вычетов всего (p-1)/2, то, (сравнение axn+a1xn-1+…+an$≡ $0(p), не все коэффициенты которого кратны p, не может иметь более, чем n решений\*), других решений у данного сравнения нет, => невычеты являются решениями сравнения (2), и требуемое доказано.

\*Предположим, что axn+a1xn-1+…+an$≡ $0(p)имеет хотя бы n+1 решение. Тогда axn+a1xn-1+…+an=a(x-x1)(x-x2)…(x-xn)+b(x-x1)…(x-xn-1­)+c(x-x1)…(x-xn-2)+…+k(x-x1)+l,где b –коэффициент при xn-1 многочлена axn+a1xn-1+…+an-a(x-x1)(x-x2)…(x-xn), с – коэффициент при xn-2 многочлена axn+a1xn-1+…+an-a(x-x1)(x-x2)…(x-xn)-b(x-x1)…(x-xn-1­)и т.д. Последовательно подставляя x1,x2,…,xn+1 вместо x получим, что l,k,…,c,b,a делятся на p, а значит, каждое из чисел a1,a2,…,an делится на p, как сумма чисел, кратных p.