JOURNAL OF NUMBER THEORY 1, 113–115 (1969)

On Factoring Quartics (mod p)*

PHILIP A. LEONARD

Department of Mathematics,
The Pennsylvania State University,
University Park, Pennsylvania 16802

Communicated by S. Chowla

Received April 1, 1968

We present a simplified proof of a theorem of Skolem. This result describes the factorization of a fourth degree polynomial (mod p), p an odd prime, in terms of its discriminant and the nature of the roots of a related resolvent cubic polynomial.

1. In [2], Skolem gave a useful criterion for describing the factorization (mod p) of monic polynomials of degree 4. The purpose of this note is to provide a simpler proof of his result, based on the cases $n = 3, 4$ of a theorem which goes back to Stickelberger. This in turn has a very simple proof (cf. [4], proof of Theorem 1).

THEOREM. *Let p be an odd prime, $f(x)$ a monic polynomial* (mod p) *of degree n, with discriminant $D(f)$ and no repeated roots. If $f(x) \equiv f_1(x) \ldots f_r(x)$* (mod p), *where each $f_i(x)$ is irreducible, then $n \equiv r$* (mod 2) *if and only if* $[D(f)/p] = 1$.

2. Consider $f(x) \equiv x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 \pmod p$, p an odd prime. Suppose that $f(x)$ has the distinct roots x_1, x_2, x_3, x_4 in its splitting field. If

$$z_1 = x_1 + x_2 - x_3 - x_4$$
$$z_2 = x_1 - x_2 + x_3 - x_4$$
$$z_3 = x_1 - x_2 - x_3 + x_4 \quad \text{and} \quad y_i = z_i^2 \ (i = 1, 2, 3),$$

then y_1, y_2, y_3 are the roots of

$$g(y) \equiv y^3 - (3a_1^2 - 8a_2)y^2 + (3a_1^4 - 16a_1^2a_2 + 16a_1a_3 + 16a_2^2 - 64a_4)y - (a_1^3 - 4a_1a_2 + 8a_3)^2$$

* This research was supported by the National Science Foundation.

Furthermore $D(g) = 2^{12}D(f)$. Since $x \to x-4^{-1}a_1$ leaves $g(y)$ and $D(f)$ unaltered, we may assume that $a_1 \equiv 0$.
Thus we have

$$g(y) \equiv y^3+8a_2y^2+(16a_2^2-64a_4)y-64a_3^2.$$

We adopt Skolem's (unstated) restriction and assume that $a_3 \not\equiv 0$. An elementary treatment of the other case is found in [*1*]. With $a_3 \not\equiv 0$, $(y_1y_2y_3/p) = (64a_3^2/p) = 1$.

3. If $f(x)$ factors into two quadratics, then we have

$$x^4+a_2x^2+a_3x+a_4 \equiv (x^2+rx+s)(x^2-rx+t),\ r \not\equiv 0.$$

Comparing coefficients gives

$$\begin{aligned} st &\equiv a_4 \\ s+t &\equiv r^2+a_2 \\ t-s &\equiv r^{-1}a_3. \end{aligned}$$

Thus

$$\begin{aligned} 2t &= r^2+a_2+r^{-1}a_3 \\ 2s &= r^2+a_2-r^{-1}a_3 \quad \text{and} \\ 4st &= 4a_4 = r^4+2r^2a_2+a_2^2-r^{-2}a_3^2. \end{aligned}$$

Therefore $r^6+2a_2^2r^4+(a_2^2-4a_4)r^2-a_3^2 \equiv 0$, or $y_1 \equiv 4r^2$ is a root of $g(y)$. Conversely, if y_1 is a root of $g(y)$ with $(y_1/p) = 1$, then $y_1 = 4r^2$, and the above equations give a factorization of $f(x)$ in the above form. The ambiguity of $^{\pm}r$ is reflected in the order of the factors. If y_1 and y_2 both have this property, the corresponding factorizations are distinct.

Remark. In applying the methods of this paper to the case $a_3 \equiv 0$, one must distinguish between $r \equiv 0$ and $r \not\equiv 0$ in factorizations of the above form.

4. We can now prove Skolem's result quite easily. In what follows, y_1, y_2, y_3 refer to distinct solutions $(\text{mod}\, p)$ of $g(y) \equiv 0$, and $D = D(f) = 2^{-12}D(g)$. There are five cases to consider:

(a) $(y_1/p) = 1$, y_2, y_3 do not exist. Then $g(y)$ has 2 factors, so $(D/p) = -1$. Hence $f(x)$ has an odd number of factors and is the product of quadratics in one way. Thus $f(x) \equiv (x-x_1)(x-x_2)h(x)$, $h(x)$ an irreducible quadratic.

(b) $(y_1/p) = 1$, $(y_2/p) = (y_3/p) = 1$. Then $f(x)$ has an even number of factors and three factorizations into quadratics. Thus

$$f(x) \equiv (x-x_1)(x-x_2)(x-x_3)(x-x_4).$$

(c) $(y_1/p) = 1$, $(y_2/p) = (y_3/p) = -1$. Again $f(x)$ has an even number of factors, but one factorization into quadratics. Thus $f(x) \equiv h_1(x)h_2(x)$, $h_1(x)$, $h_2(x)$ irreducible quadratics.

(d) $(y_1/p) = -1$, y_2, y_3 do not exist. Then $f(x)$ has an odd number of factors but no factorization into quadratics. Thus $f(x)$ is irreducible.

(e) y_1, y_2, y_3 do not exist. Then $f(x)$ has an even number of factors and no factorization into quadratics. Thus $f(x) \equiv (x-x_1)h(x)$, $h(x)$ an irreducible cubic.

Since in each case the converse is clear, the proof of Skolem's result is complete.

5. In an adjoining paper [3], Skolem intimated that a similar project could be carried out for quintic polynomials. He never did this, and to date the only general information on polynomials of degree $n > 4$ is provided by Stickelberger's Theorem.

References

1. Carlitz, L. Note on a quartic congruence. *Am. Math. Monthly* **63** (1956), 569–571.

2. Skolem, Th. The general congruence of 4th degree modulo p, p prime. *Norsk. Mat. Tidsskr.* **34** (1952), 73–80.

3. Skolem, Th. On a certain connection between the discriminant of a polynomial and the number of its irreducible factors mod p. *Norsk. Mat. Tidsskr.* **34** (1952), 81–85.

4. Swan, R. G. Factorization of polynomials over finite fields. *Pacific J. Math.* **12** (1962), 1099–1106.