ON A THEOREM OF AUBRY-THUE

ALFRED BRAUER AND R. L. REYNOLDS

1. Introduction. In 1913 L. Aubry [**1**] proved the following theorem:

If a and m are relatively prime, $m > 0$, and if $b/m^{\frac{1}{2}}$ is not an integer, then it is always possible to find integers x and y not both zero such that

$$ax - by \equiv 0 \pmod{m} \tag{1}$$

and $|x| < m^{\frac{1}{2}}$, $|y| < m^{\frac{1}{2}}$.

In 1917 A. Thue proved [**10**]:

If a, b and m are relatively prime, then (1) *can be solved by integers x and y such that* $|x| \leqslant m^{\frac{1}{2}}$, $|y| \leqslant m^{\frac{1}{2}}$.

This is called, in general, the Theorem of Thue. See, for instance, the books of A. Scholz [**7**, p. 45], and O. Ore [**5**, p. 268]. If $(b, m) = 1$ and m is not a square, the results of Aubry and Thue are identical. If m is a square but $b/m^{\frac{1}{2}}$ is not an integer, then Aubry's result is better than Thue's. Since Aubry published the theorem first and Thue proved it independently a little later, it should be called the Theorem of Aubry-Thue. In addition to the books mentioned above, this theorem is also proved in the book of Uspensky and Heaslet [**11**, p. 234] without mentioning either Aubry or Thue.

Actually Thue had already proved in 1915 [**9**] a more general result under certain unimportant restrictions without formulating it as a theorem. If we omit these restrictions, Thue's result can be formulated as follows:

If $a_1, a_2, \ldots, a_n$ are relatively prime, then it is possible to find integers $x_1, x_2, \ldots, x_n$ not all zero such that

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n \equiv 0 \pmod{m} \tag{2}$$

and $0 \leqslant |x_\nu| \leqslant m^{1/n}$.

In 1926 J. M. Vinogradov [**12**] *generalized* the Theorem of Aubry-Thue in another direction:

Let p be a prime $(a, p) = 1$ and k any positive integer. Then there exist relatively prime integers x and y satisfying

$$ax \equiv y \pmod{p},\ 0 < x \leqslant k,\ 0 < |y| < p/k.$$

It is clear that the corresponding theorem holds for $ax \equiv by \pmod{p}$ where $(b, p) = 1$. Moreover it follows from the proof that the modulus need not be a prime number. In the book of Scholz [**7**] this generalization of Thue is also proved.

Received February 24, 1950.

Independently Thue's Theorem was proved by De Backer [**3**] and Vinogradov's generalization by Ballieu [**2**]. Moreover Ballieu considered the case where a and m are not relatively prime, but ordinarily it will be sufficient for the applications to consider the case where $(a, m) = 1$ since by must be divisible by the g. c. d. of a and m. In a second paper De Backer [**4**] stated without proof the following theorem which is unfortunately incorrect:

If $(a, m) = 1$ and if A is any integer, then

$$ax \equiv y + A \pmod{m}$$

always has a solution for which $|x| \leqslant m^{\frac{1}{2}}$, $|y| \leqslant m^{\frac{1}{2}}$.

For instance, $2x \equiv y + 23 \pmod{47}$ has no solution. De Backer used this result to prove the following theorem:

If p is a prime and a, b, c, d are integers, then the system

$$\begin{aligned} ax + by &\equiv z \pmod{p} \\ cx + dy &\equiv u \pmod{p} \end{aligned}$$

always has a solution x, y, z, u where each is less than $p^{\frac{1}{2}}$ in absolute value.

We wish to prove the latter theorem is correct by proving the following generalization of the theorem of Aubry-Thue which also contains (2) as a special case.

The system of r linear homogeneous congruences in s unknowns $(r < s)$

$$\sum_{\sigma=1}^{s} a_{\rho\sigma} x_\sigma \equiv 0 \pmod{m} \qquad (\rho = 1, 2, \ldots, r)$$

always has a non-trivial solution for which

$$|x_\sigma| \leqslant m^{r/s} \qquad (\sigma = 1, 2, \ldots, s).$$

This result will be obtained by proving the corresponding generalization of Vinogradov's theorem.

The theorem of Aubry-Thue is used in particular for the proof of the representation of primes of form $4n + 1$ as sum of two squares and that the least kth power non-residue (mod p) with $p \equiv 1 \pmod{k}$ is less than $p^{\frac{1}{2}}$. Correspondingly, we shall use our generalisation to simplify the proof that every integer can be represented as sum of four squares and we shall prove here that for odd k and $p \equiv 1 \pmod{k}$ each of the $k - 1$ classes of kth power non-residues contains at least one element less than $p^{(k-1)/k}$. For sufficiently large p and the special case $k = 3$ a sharper bound can be obtained from Vinogradov's results [**13**] but not for $k > 3$.

Porcelli and Pall have just announced that they can prove the following theorem with the help of Farey Series:

If p is an odd prime, D a quadratic residue (mod p), g and h positive integers such that $g \leqslant p$ and $h = [p/g]$, then at least one of the numbers $1^2, 2^2, \ldots, h^2$ is congruent to one of the numbers $D, 4D, 9D, \ldots, (g-1)^2D$.

We will show this theorem is an immediate consequence of Vinogradov's theorem and that it also holds for kth power residues with even k. Finally we will generalize the theorem of Aubry-Thue for congruences with regard to a double modulus and for congruences with respect to ideals in algebraic number fields.

2. Generalization of Vinogradov's Theorem.

THEOREM 1. *Let r and s be rational integers with $r < s$ and let f_σ be positive numbers less than m ($\sigma = 1, 2, \ldots, s$) such that*

$$\prod_{\sigma=1}^{s} f_\sigma > m^r. \tag{3}$$

Then the system of r linear congruences

$$y_\rho = \sum_{\sigma=1}^{s} a_{\rho\sigma} x_\sigma \equiv 0 \pmod{m} \qquad (\rho = 1, 2, \ldots, r) \tag{4}$$

has a non-trivial solution in integers $x_1, x_2, \ldots, x_s$ such that

$$|x_\sigma| < f_\sigma \qquad (\sigma = 1, 2, \ldots, s). \tag{5}$$

Proof. Let f^*_σ be the greatest integer less than f_σ. For $\sigma = 1, 2, \ldots, s$ we choose

$$x_\sigma = 0, 1, 2, \ldots, f^*_\sigma \tag{6}$$

and obtain $\prod_{\sigma=1}^{s} (f^*_\sigma + 1)$ sets of r-tuples $(y_1, y_2, \ldots, y_r)$. By (3) we have

$$\prod_{\sigma=1}^{s} (f^*_\sigma + 1) \geqslant \prod_{\sigma=1}^{s} f_\sigma > m^r.$$

Thus it follows from Dirichlet's principle of the drawers that at least two of the r-tuples, say $(y'_1, y'_2, \ldots, y'_r)$ and $(y''_1, y''_2, \ldots, y''_r)$ will satisfy the congruences

$$y'_\rho \equiv y''_\rho \pmod{m} \qquad (\rho = 1, 2, \ldots, r). \tag{7}$$

If we denote the corresponding values of x_σ by x'_σ and x''_σ respectively, we have

$$\begin{aligned} y'_\rho &= a_{\rho 1}x'_1 + a_{\rho 2}x'_2 + \ldots + a_{\rho s}x'_s \\ y''_\rho &= a_{\rho 1}x''_1 + a_{\rho 2}x''_2 + \ldots + a_{\rho s}x''_s \end{aligned} \qquad (\rho = 1, \ldots, r).$$

Hence by (7) for $\rho = 1, 2, \ldots, r$,

$$a_{\rho 1}(x'_1 - x''_1) + a_{\rho 2}(x'_2 - x''_2) + \ldots + a_{\rho s}(x'_s - x''_s) \equiv 0 \pmod{m}.$$

If we denote $x'_\sigma - x''_\sigma$ by X_σ, then $X_1, X_2, \ldots, X_s$ are a non-trivial solution of the congruences (4) which by (6) satisfy the conditions (5).

COROLLARY 1. *Let $f(x)$ be any irreducible monic polynomial of degree n and p any prime. Let $f_1, f_2, \ldots, f_{2n}$ be positive numbers less than p such that*

$$\prod_{\nu=1}^{2n} f_\nu > p^n.$$

If $g(x)$ and $h(x)$ are given polynomials with integral rational coefficients, then we can find polynomials with integral rational coefficients:

$$\begin{aligned} \phi(x) &= u_1x^{n-1} + u_2x^{n-2} + \ldots + u_n, \\ \psi(x) &= v_1x^{n-1} + v_2x^{n-2} + \ldots + v_n, \end{aligned}$$

not both zero such that,

$$g(x)\phi(x) + h(x)\psi(x) \equiv 0 \pmod{f(x), p}, \tag{8}$$

where

$$|u_\nu| < f_\nu, \qquad |v_\nu| < f_{\nu+n} \qquad (\nu = 1, 2, \ldots, n).$$

Proof. The coefficients of $g(x)\phi(x)$ are linear forms in $u_1, u_2, \ldots, u_n$. If we divide $g(x)\phi(x)$ by the monic polynomial $f(x)$, then the coefficients of the remainder are also linear combinations of $u_1, u_2, \ldots, u_n$ with given integral rational coefficients. Similarly the remainder of $h(x)\psi(x)$ after dividing by $f(x)$ will have coefficients which are linear forms in $v_1, v_2, \ldots, v_n$ with given integral rational coefficients. In order that (8) may hold, at most n linear congruences in the $2n$ variables u_ν and v_ν must be satisfied. Hence the corollary follows at once from Theorem 1.

If $A = (a_{\rho\sigma})$ and $B = (b_{\rho\sigma})$ are matrices with integral elements, we write $A \equiv B \pmod m$ if $a_{\rho\sigma} \equiv b_{\rho\sigma} \pmod m$ for every ρ and σ.

COROLLARY 2. *Let $f_{\sigma\tau}$ and $f'_{\sigma\tau}$ be positive numbers less than m ($\sigma = 1, 2, \ldots, s$; $\tau = 1, 2, \ldots, t$) such that*

$$\prod f_{\sigma\tau} f'_{\sigma\tau} > m^{rt}.$$

Let $A = (a_{\rho\sigma})$ and $B = (b_{\rho\sigma})$ be two $r \times s$ matrices with integral rational elements and $r < 2s$. Then for every given integer t we can find integral $s \times t$ matrices $U = (u_{\sigma\tau})$ and $V = (v_{\sigma\tau})$ such that

$$AU \equiv BV \pmod m, \tag{9}$$

where

$$|u_{\sigma\tau}| < f_{\sigma\tau}, \; |v_{\sigma\tau}| < f'_{\sigma\tau}, \quad (\sigma = 1, 2, \ldots, s;\ \tau = 1, 2, \ldots, t).$$

Proof. The rt elements of AU are linear combinations of the elements of U. Hence (9) requires that rt linear congruences for the $2st$ unknown elements of U and V be satisfied.

A similar result holds for left-hand multiplication of A and B.

https://doi.org/10.4153/CJM-1951-042-6 Published online by Cambridge University Press

3. The Four Square Theorem. It is well known that it is sufficient to prove this theorem only for prime numbers p. The simplest proofs use the fact that we can find integers a and b such that

$$a^2 + b^2 + 1 \equiv 0 \pmod{p} \tag{10}$$

and the method of descent [**11**, pp. 383-6]. We wish to prove that the theorem follows easily from (10) and Theorem 1.

Let a and b satisfy (10), then the congruences

$$\begin{aligned} x &\equiv az + bt \pmod{p} \\ y &\equiv bz - at \pmod{p} \end{aligned} \tag{11}$$

have a non-trivial solution with

$$\max(|x|, |y|, |z|, |t|) < p^{\frac{1}{2}}. \tag{12}$$

It follows from (11) and (10) that

$$x^2 + y^2 \equiv (a^2 + b^2)z^2 + (a^2 + b^2)t^2 \equiv -z^2 - t^2 \pmod{p}.$$

Hence

$$x^2 + y^2 + z^2 + t^2 = Ap. \tag{13}$$

By (12), A must be equal to 1, 2, or 3. If $A = 1$, the theorem is proved. If $A = 2$, then x must be congruent (mod 2) to at least one of y, z, t say $x \equiv y$ (mod 2) and then also $z \equiv t$ (mod 2). We obtain from (13) for p the following representation as sum of four squares:

$$p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2.$$

If $A = 3$, we use a method of Sylvester [**8**]. It follows from (13) that one of x, y, z, t, say x, must be divisible by 3 and by proper choice of signs for y, z, and t we may assume that

$$y \equiv z \equiv t \pmod{3}.$$

Hence from (13)

$$p = \left(\frac{y+z+t}{3}\right)^2 + \left(\frac{x+z-t}{3}\right)^2 + \left(\frac{x-y+t}{3}\right)^2 + \left(\frac{x+y-z}{3}\right)^2.$$

This gives our representation since the parentheses are integers and hence proves our theorem.

4. The least kth power non-residues.

THEOREM 2. *If k is odd and p a prime where $p \equiv 1 \pmod{k}$, then each of the $k - 1$ classes of kth power non-residues contains at least one element which is less than $p^{(k-1)/k}$.*

Proof. Let $n_1, n_2, \ldots, n_{k-1}$ be representatives of the $k-1$ classes K_1, $K_2, \ldots, K_{k-1}$ of non-residues. We consider the system of $k-1$ congruences in k unknowns:

$$\begin{aligned} x &\equiv n_1 y_1 \pmod p \\ x &\equiv n_2 y_2 \pmod p \\ &\cdots \\ x &\equiv n_{k-1} y_{k-1} \pmod p. \end{aligned} \tag{14}$$

This system has a non-trivial solution $x, y_1, y_2, \ldots, y_{k-1}$ where each unknown is less than $p^{(k-1)/k}$ in absolute value. Since -1 is a kth power residue for odd k, then x and $-x$ belong to the same class. Hence we only have to show that $x, y_1, y_2, \ldots, y_{k-1}$ are representatives of the k classes of residues and non-residues. If x belongs to the class K of residues or non-residues, then y_i belongs to the class $K K_i^{-1}$ $(i = 1, 2, \ldots, k-1)$. It is obvious that these classes are different from each other and different from K.

If we consider instead of the $k-1$ congruences (14) only l of them, then it follows in the same way from Theorem 1 that l of these classes of kth power non-residues contain elements which are less than $p^{l/l+1}$. Applying this successively for $l = 1, 2, \ldots, k-1$, we obtain

THEOREM 3. *If k is odd and p a prime with $p \equiv 1$ (mod k), then it is possible to find $k-1$ non-residues $d_1, d_2, \ldots, d_{k-1}$ belonging to different classes such that*

$$0 < d_\lambda < p^{\lambda/(\lambda+1)}, \qquad (\lambda = 1, 2, \ldots, k-1).$$

This gives for d_1 the well known bound for the least kth power non-residue.

5. Generalization of a Theorem of Porcelli and Pall.

THEOREM 4. *Let g and k be positive integers where k is even, p an odd prime with $p \equiv 1$ (mod k) such that $g \leqslant p$. We set $h = [p/g]$. If D is a kth power residue, then at least one of the numbers $1^k, 2^k, \ldots, h^k$ is congruent to one of the numbers $D, 2^k D, \ldots, (g-1)^k D$.*

Proof. Since D is a kth power residue, there exists an integer a such that $a^k \equiv D \pmod p$. By Theorem 1, the congruence

$$ax \equiv y \pmod p$$

has a solution for which $|x| < g$ and $|y| < h+1$ since $g(h+1) > p$. Thus

$$a^k x^k \equiv y^k \pmod p$$

and since k is even,

$$D\,|x|^k \equiv |y|^k \pmod p.$$

Since $|x|$ is one of the numbers $1, 2, \ldots, g-1$ and $|y|$ one of the numbers $1, 2, \ldots, h$, the theorem is proved.

6. A generalization for algebraic numbers.

THEOREM 5. *Let* $\mathfrak{m}$ *be an ideal of an algebraic number field and t the norm of* $\mathfrak{m}$. *Assume that t is less than the square of the smallest rational integer g of* $\mathfrak{m}$. *If* α *and* β *are two integers of the field, then the congruence*

$$\alpha x - \beta y \equiv 0 \pmod{\mathfrak{m}} \tag{15}$$

has a solution in rational integers x and y not both belonging to $\mathfrak{m}$ *such that*

$$|x| < t^{\frac{1}{2}}, \quad |y| < t^{\frac{1}{2}}. \tag{16}$$

Proof. The numbers $0, 1, 2, \ldots, [t^{\frac{1}{2}}]$ are incongruent (mod $\mathfrak{m}$) since their difference is less than g. If we choose for x and y the numbers $0, 1, 2, \ldots, [t^{\frac{1}{2}}]$, then we obtain $\{[t^{\frac{1}{2}}] + 1\}^2$ numbers $\alpha x - \beta y$, hence more than t integers of the field. At least two of them, say $\alpha x' - \beta y'$ and $\alpha x'' - \beta y''$ must be congruent (mod $\mathfrak{m}$). Hence

$$\alpha(x' - x'') - \beta(y' - y'') \equiv 0 \pmod{\mathfrak{m}}$$

and $X = x' - x''$, $Y = y' - y''$ are a solution of (15) satisfying (16), $x' - x'' \equiv 0 \pmod{\mathfrak{m}}$ implies $x' = x''$ and $y' - y'' \equiv 0 \pmod{\mathfrak{m}}$ implies $y' = y''$.

The assumptions of Theorem 5 are satisfied, for instance, if $\mathfrak{m}$ is the product of different prime ideals of degree 1 of which no two are conjugates. If, namely,

$$\mathfrak{m} = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_t$$

and $p_1, p_2, \ldots, p_t$ the prime numbers contained in these ideals, then $p_1, p_2, \ldots, p_t$ are different and

$$t = p_1 \cdot p_2 \ldots p_t.$$

On the other hand, $p_1 p_2 \ldots p_t$ is the smallest positive integer contained in $\mathfrak{m}$. The theorem holds also if some of these prime ideals but not all are of degree 2.

Note (May 4, 1951). In the meantime the paper of Porcelli and Pall has been published [6]. While in their abstract only the case $k = 2$ is mentioned. actually Theorem 4 is proved in the paper. Our proof is completely different from the proof of Porcelli and Pall.

REFERENCES

1. L. Aubry, *Un théorème d'arithmétique*, Mathesis (4), vol. 3 (1913).

2. R. Ballieu, *Sur des congruences arithmétiques*, Bulletin de la Classe des Sciences de l'Académie Royale de Belgique (5), vol. 34 (1948), 39-45.

3. S. M. De Backer, *Un théorème fundamental*, Bulletin de la Classe des Sciences de l'Académie Royale de Belgique (5), vol. 33 (1947) 632-634.

4. ——— *Solutions modérées d'un système de congruences du premier degré pour un module premier p.* Bulletin de la Classe des Sciences de l'Academie Royale de Belgique, (5) vol. 34 (1948), 46-51.

5. O. Ore, *Number theory and its history* (New York, 1948), 268.

https://doi.org/10.4153/CJM-1951-042-6 Published online by Cambridge University Press

6. P. Porcelli and G. Pall, *A property of Farey sequences*, Can. J. Math., vol. 3 (1951) 52-53.

7. A. Scholz, *Einführung in die Zahlentheorie* (Berlin, 1939).

8. J. J. Sylvester, *Note on a principle in the theory of numbers and the resolubility of any number into the sum of four squares*, Quar. J. of Math., vol. 1 (1857), 196-7; or Collected Math. Papers, vol. 2 (1908), 101-102.

9. A. Thue, *Über die ganzzahlige Gleichung* $C^n = a^m + a^{m-1}b + \ldots + ab^{m-1} + b^m$, Norske videnskaps-akademi, Oslo, Matematisk-naturvidenskapelig klasse Skrifter, No. 3 (1915).

10. ——— *Et bevis for at lignigen* $A^3 + B^3 = C^3$ *er remulig i hele fra nul forsk jellige tal* A, B, *og* B.Archiv. for Math. og Naturvid, vol. 34, No. 15 (1917).

11. J. V. Uspensky and M. A. Heaslit, *Elementary number theory* (New York, 1939).

12. J. M. Vinogradov, *On a general theorem concerning the distribution of the residues and non-residues of powers*, Trans. Amer. Math. Soc., vol. 29 (1927), 209-17.

13. ——— *On the bound of the least non-residues of nth powers*, Trans. Amer. Math. Soc. vol. 29 (1927), 218-226.

University of North Carolina