ACTA ARITHMETICA
132.2 (2008)

Lattices in $\mathbb{Z}^2$ and the congruence $xy + uv \equiv c \pmod m$

by

Anwar Ayyad (Gaza) and Todd Cochrane (Manhattan, KS)

1. Introduction. Let m be a positive integer, $\mathcal{L}$ be a lattice of points in $\mathbb{Z}^2$ of volume $\Delta(\mathcal{L}) = m$ and $\mathcal{B}_m$ be the box of points

$$\mathcal{B}_m = \{(x,y) : |x| \le \sqrt{m},\ |y| \le \sqrt{m}\}.$$

We say $\mathcal{L}$ is *well distributed* (with respect to the box $\mathcal{B}_m$) if every integer translate $(A,B) + \mathcal{B}_m$ of $\mathcal{B}_m$ contains a point of $\mathcal{L}$ other than (A,B). Minkowski's convex body theorem implies that $\mathcal{B}_m$ itself always contains a nonzero point of $\mathcal{L}$, but in general translates of $\mathcal{B}_m$ may not contain any point of $\mathcal{L}$. For instance, the points in the lattice defined by $x \equiv y \pmod m$ are not well distributed at all.

We call $\mathcal{L}$ a *congruence lattice* (mod m) if it is defined by a linear congruence $ax + by \equiv 0 \pmod m$ with $\gcd(a,b,m) = 1$. Not all lattices in $\mathbb{Z}^2$ are congruence lattices, for instance $2\mathbb{Z}^2$. However, it is not hard to show that every lattice of volume m is of the form $\lambda\mathcal{L}' = \{\lambda x : x \in \mathcal{L}'\}$ for some positive integer λ and congruence lattice $\mathcal{L}' \pmod{m/\lambda^2}$; see Lemma 1. In particular, if m is square free, then every lattice of volume m is a congruence lattice.

Our first result gives a sufficient condition for $\mathcal{L}$ to be well distributed. Let $\mathcal{R}_m$ be the following set of integer points:

$$\mathcal{R}_m = \{(x,y) : 0 \le |x| \le \sqrt{m},\ 0 \le |y| \le \sqrt{m},\\ |x| + 2|y| \ge \sqrt{m},\ 2|x| + |y| \ge \sqrt{m}\}.$$

Theorem 1. *If $\mathcal{L}$ is a congruence lattice of volume m that contains a point $(x_0,y_0) \in \mathcal{R}_m$ with* $\gcd(x_0,y_0) = 1$ *then $\mathcal{L}$ is well distributed.*

If $\mathcal{L} = \lambda\mathcal{L}'$ for some congruence lattice $\mathcal{L}'$ of volume m/λ^2 and $\mathcal{L}'$ contains a point $(x_0,y_0) \in \mathcal{R}_{m/\lambda}$ with $\gcd(x_0,y_0) = 1$, then $\mathcal{L}$ is *uniformly distributed* in the sense that every translate of $\mathcal{B}_m$ by a vector of the form $\lambda(u,v)$

2000 *Mathematics Subject Classification*: 11A07, 11H06, 11H55, 11B75.
Key words and phrases: congruences, lattices, distribution, quadratic forms.

contains a point of $\mathcal{L}$. It is an open question whether the converse of the theorem holds true.

An equivalent way of stating Theorem 1 is

Theorem 2. *Let a,b,m be integers with $m>0$ and $\gcd(a,b,m)=1$, and suppose that the congruence $ax+by\equiv 0 \pmod{m}$ has a solution $(x_0,y_0)\in\mathcal{R}_m$ with $\gcd(x_0,y_0)=1$. Then for any integer c, the linear congruence*

$$ax+by\equiv c \pmod{m} \tag{1}$$

has a nonzero solution with $|x|\le\sqrt{m}$, $|y|\le\sqrt{m}$.

We note that the size of (x,y) obtained here is nearly best possible. Indeed, if $\mathcal{B}$ is a box of points of cardinality less than m, then for some integer c, (1) has no solution in $\mathcal{B}$. We also note that we could just as well have taken $(x,y)\in(A,B)+\mathcal{B}_m$ for any $(A,B)\in\mathbb{Z}^2$.

Next we turn to the quadratic equation,

$$xy+uv\equiv c \pmod{m}. \tag{2}$$

As a consequence of Theorem 1 we show that the solutions of (2) are well distributed in the following sense.

Theorem 3. *Let A,B,C,D and c be any integers.*

(i) *If m is a prime power then congruence (2) has a solution with*

$$|x-A|\le\sqrt{m},\qquad |y-B|\le\sqrt{m},\qquad |u-C|\le\sqrt{m},\qquad |v-D|\le\sqrt{m}+1.$$

(ii) *In general, for any positive integer m congruence (2) has a solution with*

$$|x-A|\le\sqrt{m},\qquad |y-B|\le(1+[\delta/2])\sqrt{m},$$
$$|u-C|\le\sqrt{m},\qquad |v-D|\le\sqrt{m}+[\delta/2],$$

where δ is the maximum gap between reduced residues $\pmod{m}$.

For prime powers the result is essentially best possible, aside from a possible modest improvement in the constant 1 in front of $\sqrt{m}$. Indeed, for the congruence

$$xy+uv\equiv[m/2] \pmod{m}$$

there is no solution with all variables less than $\sqrt{m-1}/2$ in absolute value. For general m there is no reason to believe that the factor δ is necessary, and most likely it can be removed altogether. In any case, $\delta\ll\log^2(m)$; see [9].

For the case of prime moduli there is an altogether different approach for addressing (2) using the combinatorial methods of [4], [3], [7], [8], [6] and other works. For any subsets S, T of $\mathbb{Z}_p$ let

$$S+T=\{s+t: s\in S,\, t\in T\},\qquad ST=\{st: s\in S,\, t\in T\},$$
$$S-T=\{s-t: s\in S,\, t\in T\},\qquad nS=S+\cdots+S\quad (n \text{ times}).$$

As noted in [6], it follows from the work of Glibichuk [7] that for any sets S, T with $|S|\,|T| > 2p$, $(2S)(2T) + (2S)(2T) = \mathbb{Z}_p$ and $(2S)(2T) - (2S)(2T) = \mathbb{Z}_p$. Applied to intervals, this shows that (2) has a solution with

$$|x - A| \le M_1, \quad |u - A| \le M_1, \quad |y - B| \le M_2, \quad |v - B| \le M_2$$

for any A, B, M_1, M_2 with $M_1 M_2 > 4p$. This result was refined by Garaev and Garcia:

Theorem 4 (Garaev and Garcia [6, Theorem 4]). *Let S, T, U, V be subsets of $\mathbb{Z}_p - \{0\}$ such that $|S|\,|U| > (2+\sqrt{2})p$ and $|T|\,|V| > (2+\sqrt{2})p$. Then $(2S)(2T) + (2U)(2V) = \mathbb{Z}_p$.*

Their result implies a solution of (2) with $|x - A| < \frac{\sqrt{15}}{2}\sqrt{p}$, $|y - B| < \frac{\sqrt{15}}{2}\sqrt{p}$, $|u - C| < \frac{\sqrt{15}}{2}\sqrt{p}$, $|v - D| < \frac{\sqrt{15}}{2}\sqrt{p}$, a slightly weaker result than Theorem 3.

The advantage of the combinatorial method is that it can obtain solutions of (2) with the variables belonging to any types of subsets of sufficiently large cardinality, not necessarily intervals. The disadvantage is that the proof is not constructive. The lattice method introduced in this paper is constructive. By following the given proof one can write an efficient algorithm for obtaining the solution guaranteed by Theorem 3. Another disadvantage is that the combinatorial method has not yet been extended to work for general moduli.

As another application of Theorem 2 we consider the congruence

$$axy + buv \equiv c \pmod{p}. \tag{3}$$

Theorem 5. *For any integers a, b, c and any prime p with $p \nmid ab$, there exists a solution of (3) in integers x, y, u, v with*

$$\max\{|x|, |y|, |u|, |v|\} < \sqrt{p}.$$

If $p \mid c$ then the integers can all be taken to be nonzero.

It is an open question whether the same type of result (perhaps with a Big-O) holds for the more general congruence $Q(x, y, u, v) \equiv c \pmod{p}$, where Q is a quadratic form. For diagonal forms in four variables a nonzero solution of size $\ll \sqrt{p}\log p$ was obtained in [5]. Finally, we note that a very detailed analysis of the distribution of solutions of the congruence $xy + uv \equiv 0 \pmod{p}$ is given in [2] and [6].

2. Lemmas

Lemma 1. *Every full lattice in $\mathbb{Z}^2$ is a scalar multiple of a congruence lattice. More specifically, if $\mathcal{L}$ is a lattice of volume m and λ is the greatest common divisor of all the coordinates of all the points in $\mathcal{L}$, then $\mathcal{L} = \lambda\mathcal{L}'$ for some congruence lattice $\mathcal{L}'$ of volume m/λ^2.*

Proof. Let $(a,b),(c,d)$ be a basis of $\mathcal{L}$. Then $|ad-bc|=m$ and $\gcd(a,b,c,d)=\lambda$. If $\lambda>1$, we let $\mathcal{L}'=\lambda^{-1}\mathcal{L}$, and so we may assume $\lambda=1$. Let $A=\left[\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right]$. There exist invertible matrices $P=[p_{ij}]$, $Q=[q_{ij}]$ over $\mathbb{Z}$ such that $PAQ=\left[\begin{smallmatrix}1&0\\0&m\end{smallmatrix}\right]$. Then $A\left[\begin{smallmatrix}q_{12}\\q_{22}\end{smallmatrix}\right]\equiv\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\pmod{m}$, and so $\mathcal{L}\subset\mathcal{L}_1$, where $\mathcal{L}_1$ is the solution set of $q_{12}x+q_{22}y\equiv 0\pmod{m}$. Now since $\gcd(q_{12},q_{22})=1$, $\mathcal{L}_1$ is also of volume m. Thus $\mathcal{L}=\mathcal{L}_1$. ∎

Lemma 2. *Let a,b,m be positive integers with* $\gcd(a,b)=1$, *and c be any integer. There is a solution of* (1) *with*

$$|x|\le\frac{1}{2}\left(b+\max\left\{\frac{m+ab}{a+b},\frac{|m-b^2|}{a+b}\right\}\right),$$
$$|y|\le\frac{1}{2}\left(a+\max\left\{\frac{m+ab}{a+b},\frac{|m-a^2|}{a+b}\right\}\right).$$

The lemma is a variant of [1, Theorem 2] suited for the special case we need here.

Proof. We start by obtaining a small integer point on the line $ax+by=m$. Put $M=(m+ab)/(a+b)$,

$$(x_1,y_1)=\left(\frac{m-bM}{a},M\right)=\left(\frac{m-b^2}{a+b},\frac{m+ab}{a+b}\right),$$
$$(x_2,y_2)=\left(M,\frac{m-aM}{b}\right)=\left(\frac{m+ab}{a+b},\frac{m-a^2}{a+b}\right).$$

Then (x_1,y_1), (x_2,y_2) are on the line and $|x_2-x_1|=x_2-x_1=b$. Since the x-coordinates of integer points on the line are b units apart, there exists an integer point on the line between (x_1,y_1) and (x_2,y_2), that is, there is an integer point (x_0,y_0) on the line with

$$\frac{m-b^2}{a+b}\le x_0\le\frac{m+ab}{a+b},\qquad \frac{m-a^2}{a+b}\le y_0\le\frac{m+ab}{a+b}.$$

Let $\mathcal{L}$ be the lattice of solutions of the congruence $ax+by\equiv 0\pmod{m}$, of volume m. Since $ax_0+by_0=m$, the points $(b,-a)$, (x_0,y_0) form a basis for $\mathcal{L}$. Since $\gcd(a,b)=1$, we have $ax+by=c$ for some integer pair (x,y). Now there exists an integer pair (u,v) such that $(x,y)\equiv(u,v)\pmod{\mathcal{L}}$ with $(u,v)=\alpha(b,-a)+\beta(x_0,y_0)$ for some real α,β with $|\alpha|\le 1/2$, $|\beta|\le 1/2$. Then (u,v) is a solution of (1) satisfying the conditions of the lemma. ∎

Lemma 3. *Let m be any positive integer and $(a,b)\in\mathcal{R}_m$ with* $\gcd(a,b)=1$. *Then for any integer c,* (1) *has a solution with $|x|\le\sqrt{m}$, $|y|\le\sqrt{m}$.*

Proof. We may assume a and b are nonnegative. Since $0\le b\le m$, we have $0\le m-b^2\le m+ab$. Let (x,y) be the solution given by Lemma 2.

Then $|x| \le \sqrt{m}$ if $b + (m + ab)/(a + b) \le 2\sqrt{m}$, that is,

$$b^2 + (2a - 2\sqrt{m})b + m - 2a\sqrt{m} = (b - \sqrt{m})(b - \sqrt{m} + 2a) \le 0,$$

or $\sqrt{m} - 2a \le b \le \sqrt{m}$. The latter follows from $(a, b) \in \mathcal{R}_m$. By symmetry we also get $|y| \le \sqrt{m}$. ■

3. Proofs of Theorems 1 and 2

Proof of Theorem 2. Let a, b, m be integers with $m > 0$ and $\gcd(a, b, m) = 1$, say $\alpha a + \beta b + \mu m = 1$ for some integers α, β and μ. Let $(x_0, y_0) \in \mathcal{R}_m$ be such that $\gcd(x_0, y_0) = 1$ and $ax_0 + by_0 \equiv 0 \pmod{m}$. Put $\lambda = \alpha y_0 - \beta x_0$. Then

$$\lambda a \equiv y_0 \pmod{m}, \qquad \lambda b \equiv -x_0 \pmod{m}, \qquad \gcd(\lambda, m) = 1.$$

Since $(y_0, -x_0) \in \mathcal{R}_m$ and $\gcd(y_0, x_0) = 1$, it follows from Lemma 3 (with (a, b) replaced by $(y_0, -x_0)$) that the congruence

$$\lambda ax + \lambda by \equiv \lambda c \pmod{m}$$

has a nonzero solution with $|x| \le \sqrt{m}$ and $|y| \le \sqrt{m}$. Since $\gcd(\lambda, m) = 1$, this is a solution of (1). ■

Proof of Theorem 1. Let $\mathcal{L}$ be a congruence lattice of volume m defined by $ax + by \equiv 0 \pmod{m}$ with $\gcd(a, b, m) = 1$. Let (A, B) be any pair of integers. If $\mathcal{L}$ contains a point $(x_0, y_0) \in \mathcal{R}_m$ with $\gcd(x_0, y_0) = 1$ then by Theorem 2 the congruence

$$a(A + x) + b(B + y) \equiv 0 \pmod{m}$$

has a nonzero solution with $|x| \le \sqrt{m}$, $|y| \le \sqrt{m}$, and we are done. ■

4. Proofs of Theorems 3 and 5

Proof of Theorem 3. Let m, A, B, C, D, c be any integers with $m > 0$. Let $\mathcal{L}$ be the lattice defined by $y \equiv [\sqrt{m}]x \pmod{m}$. Since $(1, [\sqrt{m}]) \in \mathcal{R}_m \cap \mathcal{L}$ and $\gcd(1, [\sqrt{m}]) = 1$, it follows from Theorem 1 that $\mathcal{L}$ contains a point (y_0, v_0) with $|B - y_0| \le \sqrt{m}$ and $|D - v_0| \le \sqrt{m}$, say

$$\lambda(1, [\sqrt{m}]) \equiv (y_0, v_0) \pmod{m}$$

for some integer λ. We consider solving the linear congruence

$$xy_0 + uv_0 \equiv c \pmod{m}. \tag{4}$$

Since $y_0 \equiv [\sqrt{m}]v_0 \pmod{m}$, the congruence $xy_0 + uv_0 \equiv 0 \pmod{m}$ has solution $(1, -[\sqrt{m}]) \in \mathcal{R}_m$. Thus by Theorem 2, (4) has a solution (x_0, u_0) with $|A - x_0| \le \sqrt{m}$, $|C - u_0| \le \sqrt{m}$, provided that $\gcd(y_0, v_0, m) = 1$.

If $\gcd(y_0, v_0, m) > 1$ then we let μ be the integer of smallest modulus such that $\gcd(\mu[\sqrt{m}] + y_0, \mu + v_0, m) = 1$, replace (y_0, v_0) by $(\mu[\sqrt{m}] + y_0, \mu + v_0)$, and proceed as above. Thus we obtain a solution of (2) with $|B - y_0| \le$

$(1+|\mu|)\sqrt{m}$ and $|D-v_0| \le \sqrt{m}+|\mu|$. If δ is the maximum gap between consecutive reduced residues (mod m) then we have $|\mu| \le [\delta/2]$. If m is a prime power (so that $\delta = 2$) we take μ to be 1 if $y_0 < 0$ and $\mu = -1$ if $y_0 > 0$ to obtain the bound in part (i). ■

Proof of Theorem 5. We start by multiplying the congruence (3) by an appropriate constant to make the coefficients a, b small. Let $\mathcal{L}$ be the lattice of points in $\mathbb{Z}^2$ given by

$$\{(x,y) \in \mathbb{Z}^2 : (x,y) \equiv \lambda(a,b) \pmod{p} \text{ for some } \lambda \in \mathbb{Z}\}.$$

Since (a,b) is a nonzero vector (mod p), $\mathcal{L}$ is a lattice of volume p and so, by Minkowski's convex body theorem, there is a nonzero $(x,y) \in \mathcal{L}$ with $|x|, |y| \le \sqrt{p}$, say $(x,y) \equiv \lambda(a,b) \pmod{p}$. Multiplying (3) by λ yields a new congruence of the same type with $p \nmid ab$ and $|a|, |b| < \sqrt{p}$.

Set $y = b$, and multiply the congruence by the multiplicative inverse of b (mod p) to obtain a congruence of the type

$$ax + uv \equiv c \pmod{p} \tag{5}$$

with $0 < a < \sqrt{p}$ (replacing x with $-x$ in case $a < 0$). If $c \equiv 0 \pmod{p}$ one readily obtains a small solution of (3) with all variables nonzero by taking $x = 1$, $u = a$, $v = -1$.

Let α be any integer with $0 \le \alpha < a$ and $\gcd(a, [\sqrt{p}] - \alpha) = 1$. There are $\phi(a)$ choices for α. Put $u = [\sqrt{p}] - \alpha$ and consider the congruence

$$ax + ([\sqrt{p}] - \alpha)v \equiv c \pmod{p}. \tag{6}$$

Since $(a, [\sqrt{p}] - \alpha) \in \mathcal{R}_p$, it follows from Theorem 2 that (6) has a nonzero solution with $|x| < \sqrt{p}$ and $|v| < \sqrt{p}$. ■

Acknowledgements. The authors wish to thank Sergei Konyagin for correcting our upper bound for δ and noting reference [9].

References

[1] A. Ayyad, *The geometry of solutions of the congruence* $ax \equiv by+c \pmod{p}$, preprint.

[2] A. Ayyad, T. Cochrane and Z. Zheng, *The congruence* $x_1x_2 \equiv x_3x_4 \pmod{p}$, *the equation* $x_1x_2 = x_3x_4$, *and mean values of character sums*, J. Number Theory 59 (1996), 398–413.

[3] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) 73 (2006), 380–398.

[4] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields and their applications*, Geom. Funct. Anal. 14 (2004), 27–57.

[5] T. Cochrane and Z. Zheng, *Small solutions of the congruence* $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \equiv c \pmod{p}$, Acta Math. Sinica (N.S.) 14 (1998), 175–182.

[6] M. Z. Garaev and V. C. Garcia, *The equation* $x_1x_2 = x_3x_4 + \lambda$ *in fields of prime order and applications*, preprint, 2007.

[7] A. A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime and the Erdős–Graham problem*, Mat. Zametki 79 (2006), 384–395 (in Russian); English transl.: Math. Notes 79 (2006), 356–365.

[8] A. A. Glibichuk and S. V. Konyagin, *Additive properties of product sets in fields of prime order*, arXiv:math/0702729v1, 2007.

[9] H. Iwaniec, *On the problem of Jacobsthal*, Demonstratio Math. 11 (1978), 225–231.

Department of Mathematics
Al Azhar University
P.O. Box 1277
Gaza Strip, Palestine
E-mail: anwarayyad@yahoo.com

Department of Mathematics
Kansas State University
Manhattan, KS 66506, U.S.A.
E-mail: cochrane@math.ksu.edu

Received on 1.8.2007
and in revised form on 18.12.2007 (5491)