THE DISTANCE BETWEEN UNITS IN RINGS - AN ALGORITHMIC APPROACH

Douglas Stinson

ABSTRACT. Given a finite set of positive prime integers $P = \{p_1, \ldots, p_n\}$, define $U(P)$ to be the smallest positive integer δ such that, given any δ consecutive positive integers, at least one of them is divisible by no p_i, $1 \le i \le n$. An algorithm which facilitates evaluation of $U(P)$ is described. Also, values $U(P_k)$ are obtained, where $P_k = \{q \le k,\ q \text{ prime}\}$, for $k < 50$.

1. *Introduction.*

Suppose P is a finite set of positive prime integers. Define $U(P)$ to be the smallest positive integer δ such that, given any positive integer n, there exists an integer t such that $n \le t < n + \delta$ and $(t,p) = 1$ for every $p \in P$. As is usual, (a,b) denotes the greatest common divisor of positive integers a and b.

Let $p^* = \prod_{p \in P} p$. Then $(a + kp^*, p) = (a,p)$ for all positive integers a and k, and for any $p \in P$. For a positive integer n, let Z_n denote the ring of integers modulo n. A *unit* in Z_n is any invertible element. Then, in view of the remark above, the desired value $U(P)$ may be described as the maximum distance between "consecutive" units of Z_{p^*}. Since 1 is a unit of Z_{p^*}, we have immediately that $U(P) \le p^*$, thus guaranteeing that $U(P)$ is finite.

Let $P_k = \{q \le k,\ q \ \text{prime}\}$. The values $U(P_k)$ are of particular interest in the study of mutually orthogonal Latin squares (MOLS), as we now demonstrate.

A *Latin square* L of order n is an n by n array of elements of an n-set $S(L)$ such that the elements in any row or column of L comprise the totality of $S(L)$. Two Latin squares L and M of order n are said to be *orthogonal* if, given any ordered pair $(\ell,m) \in S(L) \times S(M)$, there exists a unique cell (i,j) such that $\ell \in L(i,j)$ and $m \in M(i,j)$. Several Latin squares of order n are said to be *mutually orthogonal* if each pair of squares is orthogonal.

The following is a fundamental result of MacNeish [2].

UTILITAS MATHEMATICA Vol. 16 (1979), pp. 281-292.

THEOREM 1.1 *If* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *is the factorization of* n *into prime powers, there exist at least* $\min_{1 \le i \le k} \{p_i^{\alpha_i} - 1\}$ *MOLS of order* n.

We may now prove

THEOREM 1.2. *Let* k *be a positive integer. Then given any positive integer* n, *there exists an integer* t *such that* $n \le t < n + U(P_k)$ *and there exist* k *MOLS of order* t.

Proof. If $(t,p) = 1$ for $p \in P_k$ then there exist k MOLS of order t by Theorem 1.1. The existence of such t is guaranteed by the definition of $U(P)$.

Theorem 1.2, or special cases of it, is used in proofs of the existence of MOLS. See, for example Wilson [5] or Mullin et al. [3].

2. *A Method to Evaluate* $U(P)$.

We will depend fundamentally on the Chinese Remainder Theorem, proven in many textbooks, e.g. Schilling and Piper [4]. We state it here as a lemma.

LEMMA 2.1. *Let* $m_1, \ldots, m_n$ *be* n *pairwise relatively prime integers, each greater than* 1, *and let* $a_1, \ldots, a_n$ *be* n *arbitrary integers. Then the system of* n *congruences*

$$x \equiv a_i \bmod m_i, \quad 1 \le i \le n ,$$

has a unique solution modulo $m^* = \prod_{j=1}^{n} m_j$.

We now present several definitions. Suppose P, and p^* are as described in Section 1. Let $P = Q \cup R$, where $Q \cap R = \emptyset$. Denote $q^* = \prod_{q \in Q} q$, $r^* = \prod_{r \in R} r$. Then $p^* = q^* r^*$. For a finite set A of positive integers, let $U(A) = \{x \in Z \mid (x,a) = 1$ if $a \in A\}$, let $U_a^b(A) = \{u \in U(A) \mid a \le u \le b\}$. If $A \subseteq B$, let $B - A = \{b \mid b \in B, b \notin A\}$. Now, let B be a finite set of pairwise relatively prime integers greater than 1. Define a *congruence assignment*, or CA, on B to be a function f such that $f(b) \in Z_b$ for every $b \in B$. Define a *partial congruence assignment*, or PCA, on B to be a CA on S(f), for some $S(f) \subseteq B$. Let CA(B) and PCA(B) denote respectively the set of all CAs and PCAs on B.

For $x \in \mathcal{U}_1^{q*}(Q)$ (equivalently, for each unit of Z_{q*}) and $f \in PCA(R)$, let x(f) satisfy

(1) $x(f) \equiv x$ modulo $q*$;

(2) $x(f) \equiv f(r)$ modulo r for each $r \in S(f)$;

(3) $0 \le x(f) < q*(r')*$, where $(r')* = \prod_{r' \in S(f)} r'$.

By Lemma 2.1, x(f) satisfying (1) and (2) exists and is unique modulo $q*(r')*$; thus (3) determines x(f) uniquely.

We now define several functions based on the concepts defined above.

Suppose $f \in PCA(R)$ and x and y are positive integers with $y \le x$. Let $\mathcal{U}_x^y(f,q) = \left\{u \in \mathcal{U}_x^y(Q) \mid u - x \not\equiv -f(r) \text{ modulo } r, \text{ for every } r \in S(f)\right\}$. Let $u(x,f,\delta) = |\ \mathcal{U}_x^{x+\delta}(f,Q)\ |$, and let $v(f) = |R - S(f)|$. Finally let $t(x,f,\delta) = v(f) - u(x,f,\delta)$. We are now able to prove the following lemma.

LEMMA 2.2. *Suppose* $f \in PCA(R)$, $x \in \mathcal{U}_1^{q*}(Q)$, *and* δ *is a positive integer. If* $t(x,f,\delta) \ge 0$, *then there exists an integer* y *such that*

(1) $y \equiv x$ modulo $q*$,

(2) $(t,p*) > 1$ *if* $y \le t \le y + \delta$.

Proof. Let $A = \{a_1,\ldots,a_j\} = \mathcal{U}_x^{x+\delta}(f,Q)$. Then, by assumption, $j \le v(f)$. Let $g: A \to R - S(f)$ be any one-to-one function. Let $T = S(f) \cup g(A)$ and define $h \in PCA(R)$ by

$$h(r) = \begin{cases} f(r) & \text{if } r \in S(f) \\ x - g(s) & \text{if } s \in g(A) \end{cases}.$$

Then $S(h) = T$. Let $y = x(h)$. Then $y \equiv x(f)$ modulo $q*(r')*$ so $y \equiv x$ modulo q. Also, by the choice of g, $(t,p*) > 1$ if $y \le t \le y + \delta$.

As an example, suppose $P = \{2,3,5,7,11,13,17,19,23,29\}$, $Q = \{2,3,5,7\}$, $R = P - Q$, $x = 37$, $\delta = 33$, and $f(11) = 0$, $f(13) = 9$, so $S(f) = \{11,13\}$. Then $\mathcal{U}_x^{x+\delta}(Q) = \{37,41,43,47,53,59,61,67\}$, and

$\mathcal{U}_x^{x+\delta}(f,Q) = \{43,47,53,61\}$. Thus $u(x,f,\delta) = 4$, $v(f) = 4$, so $t(x,f,\delta) = 0$. Applying Lemma 2.2, we see that there exists $y \equiv 37$ modulo 210, such that $(t,p) > 1$ if $y \leq t \leq y + 33$ and, p prime, $p \leq 29$.

The following lemma describes the behaviour of t.

LEMMA 2.3. *Suppose* $x \in \mathcal{U}_1^{q*}(Q)$, $f \in PCA(R)$, *and* $\delta \geq 0$. *Then* $t(x,f,\delta) \geq t(x,f,\delta + 1) \geq t(x,f,\delta) - 1$.

Proof. The proof is immediate.

For $x \in \mathcal{U}_1^{q*}(Q)$ and $f \in PCA(R)$ define $\beta(x,f) = \max\{\delta \mid t(x,f,\delta) \geq 0\}$. Since t is monotonic and decreases by unit increments (Lemma 2.3), we have $0 = t(x,f,\beta(x,f))$ and $-1 = t(x,f,\beta(x,f) + 1)$. In the example, it may be checked that $t(x,f,\delta + 1) = -1$, so $\beta(x,f) = \delta = 33$.

Now define $\gamma(x) = \max\limits_{f \in PCA(R)} \{\beta(x,f)\}$.

We relate $\gamma(x)$ to the distance between units modulo $p*$ as follows.

LEMMA 2.4. *Suppose* $x \in \mathcal{U}_1^{q*}(Q)$. *Let* $\delta_0 = \alpha(x)$. *Then there exists* $y_0 \equiv x$ modulo $q*$ *such that* $(t,p*) > 1$ *if* $y_0 \leq t \leq y_0 + \delta_0$. *Further, for any* $y_1 \equiv x$ modulo $q*$ *there exists* t *such that* $y_1 \leq t \leq y_1 + \delta_0 + 1$ *and* $(t,p*) = 1$.

Proof. Let $\beta(x,f_0) = \delta_0 = \gamma(x)$. Then $t(x,f_0,\delta_0) \geq 0$. By Lemma 2.2, there exists y_0 with the required properties. Now suppose, for some y_1, that $y_1 \equiv x$ modulo $q*$ and $(t,p*) > 1$ if $y_1 \leq t \leq y_1 + \delta_0 + 1$. Define $f_1 \in PCA(R)$ by $f_1(r) \equiv y_1$ modulo r, for each $r \in R$. Then $\beta(x,f_1) > \delta_0$, a contradiction.

Let $x'(x) = \max\{y \mid y < x, (y,q) = 1\}$ and let $\varepsilon(x) = x - x'(x)$. Then we have

THEOREM 2.5. $U(P) = \max\limits_{x \in \mathcal{U}^{q*}(Q)} \{\gamma(x) + \varepsilon(x)\}$.

Proof. Let $x_0 \in \mathcal{U}_1^{q*}(Q)$ maximize $\gamma(x) + \varepsilon(x)$. Let $\delta_0 = \beta(x,f_0) = \gamma(x_0)$. Then by Lemma 2.4, there exists y_0 such that $y_0 \equiv x_0$ modulo $q*$ and $(t,p*) > 1$ if $y_0 \le t \le y_0 + \delta_0$. Let $y_1 = y_0 - \varepsilon(x)$. Then, by the definition of $\varepsilon(x)$, we have $(t,q*) > 1$ if $y_1 \le t \le y_0$ since $q*|p*$, we have $(t,p*) > 1$ if $y_1 \le t \le y_0 + \delta$. Since $y_0 + \delta - y_1 = \gamma(x_0) + \varepsilon(x_0)$, we have

$$U(P) \ge \max_{x \in \mathcal{U}_1^{q*}(Q)} \{\gamma(x) + \varepsilon(x)\} .$$

Now suppose there exists y_0 such that $(t,p*) \ge 1$ if $y_0 < t < t + \delta$ for some $\delta > \gamma(x_0) + \varepsilon(x_0)$. Let $y_1 = \min\{z | z \ge y_0, (z,q*) = 1\}$. We may assume that $y_0 = x'(y_1)$ (this can only increase the number of consecutive non-units modulo $p*$). Let $x_1 \equiv y_1$ modulo $q*$, $x_1 \in \mathcal{U}_1^{q*}(Q)$. Now, $\varepsilon(x_1) + \gamma(x_1) < \delta$, so we apply Lemma 2.4 with $\delta_0 = \delta - \varepsilon(x_1) - 1$. Then there exists t such that $y_1 \le t \le y_1 + \delta_0 + 1$ and $(t,p*) = 1$. But $y_1 + \delta_0 + 1 = y_0+\delta$, so we have a contradiction.

The problem with the above description of $U(P)$ is that $\gamma(x)$ is difficult to evaluate. We now describe a more efficient method to evaluate γ, by taking the maximum value of $\beta(x,f)$ over a (relatively) small subset of PCA(R).

Suppose $f,f' \in$ PCA(R) and $x \in \mathcal{U}_1^{q*}(Q)$. We will say that $f \le f'$ if $S(f) \subseteq S(f')$ and $f(r) = f'(r)$ if $r \in S(f)$. We say that $f < f'$ if $f \le f'$ and $S(f) \ne S(f')$. We now define a *strong* PCA as follows. If $S(f) = \emptyset$ then f is strong. Further, if f is strong, $f < f'$, $|S(f')| = |S(f)| + 1$, and $\beta(x,f') > \beta(x,f)$, then f' is strong. We say that f is *maximal* if f is strong and there does not exist f' such that $f < f'$ and f' is strong. It would be more precise to say that a PCA is strong or maximal with respect to a certain $x \in \mathcal{U}_1^{q*}(Q)$, but in all cases the value of x will be understood, so we use strong and maximal for simplicity.

The following lemma states that, in evaluating $\gamma(x)$, only strong PCAs need be considered.

LEMMA 2.6. *Suppose* $f \in$ PCA(R). *Then there exists* $f' \in$ PCA(R) *such that* $f' \le f$, f' *is strong, and* $\beta(x,f') \ge \beta(x,f)$.

Proof. Suppose $x \in U_1^{q^*}(Q)$, $f \in PCA(R)$, and $r \in R$. Define $h(x,f,r) = \max\{\delta \mid$ there do not exist $a_1, a_2 \in U_x^{x+\delta}(f,Q)$ such that $a_1 \neq a_2$ and $r \mid (a_1 - a_2)\}$. If $r \in S(f)$, let f_r be defined $f_r(r') = f(r')$ if and only if $r' \in S(f) - \{r\}$. Thus $S(f_r) = S(f) - \{r\}$. Let $\alpha(x,f) = \min_{r \in S(f)} \{h(x,f_r,r)\}$

In what follows we may assume $S(f) \neq \emptyset$. We have two cases.

Case (1). $\alpha(x,f) < \beta(x,f)$. We will show that f is strong. Let $S(f) = \{r_1, \ldots, r_\ell\}$, where $h(x,f_{r_i},r_i) < h(x,f_{r_j},r_j)$ if $i < j$ (certainly no two of these h's are equal). Let us define a sequence of PCAs as follows: f_0 is the empty PCA, and $f_k(r_i) = f_{k-1}(r_i)$ if $i \leq k-1$, $f_k(r_k) \equiv x - h(x,f_{r_k},r_k)$ modulo r_k if $1 \leq i \leq \ell$. Then $f = f_\ell$. Now, for any i such that $1 \leq i \leq \ell$, $S(f_i) = S(f_{i-1}) \cup \{r_i\}$ where $r_i \notin S(f_{i-1})$, and $f_{i-1} < f_i$. Thus we need only show that $\beta(x,f_{i-1}) < \beta(x,f_i)$. We have $v(f_i) = v(f_{i-1}) + 1$. Let $\delta = \beta(x,f_i)$. Then $u(x,f_i,\delta) \geq u(x,f_{i-1},\delta) + 2$. Then $0 = t(x,f_i,\delta) \geq t(x,f_{i-1},\delta) + 1$, and $\beta(x,f_{i-1}) < \beta(x,f_i)$, as required.

Case (2). $\alpha(x,f) \geq \beta(x,f)$. Suppose $h(x,f_{r'},r') < \beta(x,f)$ for some $r' \in S(f)$. Define $f_1 < f$ by $f_1(r) = f(r)$ if $r \in S(f) - \{r\}$. It is easy to check that $\beta(x,f_1) \geq \beta(x,f)$. Now if $\alpha(x,f_1) < \beta(x,f_1)$, Case (1) applies and f_1 is strong. Otherwise, we continue, and obtain a sequence of PCAs $f = f_0, f_1, f_2, \ldots, f_m$ where $f_j > f_{j+1}$, $S(|f_{j+1}|) = S(|f_j|) - 1$, $\beta(x,f_j) \geq \beta(x,f_{j-1}) \geq \beta(x,f)$, and $\alpha(x,f_j) \geq \beta(x,f_j)$ for $1 \leq j \leq m$. Eventually we must have $\alpha(x,f_n) < \beta(x,f_n)$ for some positive integer n, whence we may apply Case (1); or $S(f_n) = \emptyset$. However in this case as well, f_n is strong, so we are finished.

Thus we may redefine γ.

THEOREM 2.7. $\gamma(x) = \max_{f \in PCA(R)} \{\beta(x,f) \mid f$ is maximal$\}$.

Proof. Let $f_0 \in PCA(R)$ satisfy

(1) f_0 is maximal, and

(2) if f is maximal, then $\beta(x,f_0) \geq \beta(x,f)$.

Since $f_0 \in PCA(R)$ we certainly have $\beta(x,f_0) \le \gamma(x)$. Let $\gamma(x) = \beta(x,f_1)$. Then by Lemma 2.6, there exists $f_2 \in PAC(R)$ such that f_2 is strong and $\beta(x,f_2) \ge \beta(x,f_1)$. If f_2 is not maximal, there exists a maximal $f_3 \in PCA(R)$ such that $f_2 \le f_3$. Then $\beta(x,f_3) \ge \beta(x,f_2) \ge \beta(x,f_1)$. By definition of f_0, $\beta(x,f_0) \ge \beta(x,f_3) \ge \gamma(x)$, giving the reverse inequality.

To illustrate, let us return to the example described earlier. With P,Q,R,x as defined, we will evaluate $\gamma(x)$, speaking informally. Starting at 37, the units modulo 210 are 37,41,43,47,53,59,61,67,71,... . We are interested in numbers from the above list whose difference is divisible by a member of R, in order to obtain strong PCAs. For example, we have $11|(59-37)$, and $13|(67-41)$. It is easy to check that the following are the only strong PCAs.

$$\begin{aligned}
&(1) \quad f_1 = \text{"null PCA"},\\
&(2) \quad f_2(11) \equiv 0 \text{ modulo } 11,\\
&(3) \quad f_3(11) \equiv 0 \text{ modulo } 11,\\
&\qquad\; f_3(13) \equiv 9 \text{ modulo } 13.
\end{aligned}$$

Of these, only f_3 is a maximal PCA. Thus $\gamma(37) = \beta(37,f_3) = 33$. We may represent this maximum PCA as follows:

37	41	43	47	53	59	61	67
11	13	0	0	0	11	0	13

The first line lists units modulo 210 , and the second line lists elements of R by which the corresponding units may be divisible, as determined by the PCA f which maximizes $\beta(x,f)$, or a zero where that unit would be divisible by some $r \in R - S(f)$. Of course, the Chinese Remainder Theorem could be used to solve the system of congruences, if desired.

Here, we could solve, for example,

$$\begin{aligned}
y &\equiv 37 \text{ modulo } 210\\
y &\equiv 0 \text{ modulo } 11\\
y &\equiv 9 \text{ modulo } 13\\
y &\equiv 11 \text{ modulo } 17\\
y &\equiv 9 \text{ modulo } 19\\
y &\equiv 7 \text{ modulo } 23\\
y &\equiv 5 \text{ modulo } 29
\end{aligned}$$

To obtain $U(29)$, one could repeat the above procedure for each unit modulo 210.

3. *An Algorithm for the Evaluation of* γ.

We now have all the necessary machinery to produce an algorithm to evaluate γ. We will be slightly more informal in describing the algorithm than we have been while developing the theory. We also emphasize that we do not intend to describe the algorithm in complete detail, but rather give an idea of how the preceding theory can be used to obtain an efficient algorithm suitable to be programmed on a computer.

We first describe a procedure, or subroutine, which accepts as input a strong PCA and attempts to "extend" it. We refer to this procedure as EXTEND,

Input: $x \in \mathcal{U}_1^{Q^*}(Q)$, a strong PCA f, the sets Q, R, and $\delta=\beta(x,f)$.

Output: (1) A vector $M(i)$, $1 \le i \le n$ (for some integer n, which may equal zero, in which case M is empty).

(2) A vector $RES(i)$, $i \le i \le n$.

For any i, $1 \le i \le n$, $M(i) \in R - S(f)$ and $RES(i)$ denotes a residue molulo $M(i)$. We require that the following property (*) be satisfied:
(*) Let $f_i \in PCA(R)$ be defined: $f_i(r) = f(r)$ if $r \in S(f)$ and $f_i(M(i)) \equiv RES(i)$ modulo $M(i)$. Then f_i is strong.

Also, we wish M and RES to contain all possible ways of extending f to an f_i which enjoys (*).

EXTEND

(1) Set $n = 0$, $mod = 1$, $i = 1$, $j = 2$ (mod will index $R - S(f)$, which we denote by B, from 1 to m, say; i and j will determine all unordered pairs of elements from $\mathcal{U}_x^{x+\delta}(f,Q)$, say $1 \le i < j \le k$. We will denote $\mathcal{U}_x^{x+\delta}(f,Q)$ by A).

(2) If $B(mod)$ divides $A(j) - A(i)$ go to (5).

(3) Set $j = j - 1$. If $j > k$ set $i = i +1$, $j = i + 1$. If $i \ge k$ go to (4); otherwise, go to (2).

(4) Set $mod = mod + 1$. If $mod > m$, return. Otherwise set $i = 1$, $j = 2$, go to (2).

(5) Set $n = n + 1$, $M(n) = B(\text{mod})$, $RES(n) \equiv x - A(i)$ modulo $M(n)$ go to (3).

We now incorporate EXTEND into a backtrack algorithm GAMMA, which naturally enough evaluates $\gamma(x)$, given $x \in \mathcal{U}_1^{q*}(Q)$.

Input: The sets Q, R, $\mathcal{U}_1^{q*}(Q)$, and $x \in \mathcal{U}_1^{Q*}(Q)$.

Output: $\gamma(x)$ and a PCA f for which $\beta(x,f) = \gamma(x)$.

GAMMA

(1) Set lev = 0, f = "null PCA", fmax = "null PCA", $\gamma = 0$.
Notes: (a) Lev will equal the number of elements in $S(f)$.
(b) Because we will be checking several maximal PCAs we must keep a record of the maximum PCA throughout the backtrack.

(2) Determine $\beta(x,f)$.

(3) Call EXTEND (the values of n obtained are stated in a vector, subscripted as $n(\text{lev} + 1)$).

(4) If $n(\text{lev} + 1) = 0$, go to (7).

(5) Set lev = lev + 1, c(lev) = 1 (c is a "counter" vector).

(6) EXTEND f to f_i, as described in EXTEND, where $i = c(\text{lev})$; go to (2).

(7) (Here f is maximal.) If $\beta(x,f) \leq \gamma(x)$ go to (9).

(8) Set $f_{max} = f$, $\gamma = \beta(x, f_{max})$.

(9) Set $c(\text{lev}) = c(\text{lev}) + 1$. If $c(\text{lev}) \leq n(\text{lev})$ go to (6).

(10) Set lev = lev - 1. "Cut back" on f by eliminating the last "extension" in step (6).

(11) If lev = 0 stop; otherwise go to (9).

Comments. (1) Actually, a list of vectors M and RES must be stored according to the value of lev when they were calculated, in order that steps (6) and (10) may be carried out. That is, M and RES should be doubly subscripted. To simplify the description of the algorithm, we have omitted the necessary "cataloguing" procedures

(2) Calculation of $\beta(x,f)$ is straightforward, and we do not describe it in detail.

(3) Given the procedure GAMMA, it is a simple matter to determine $\max_{x \in \mathcal{U}_1^{q*}(Q)} \{\gamma(x) + \varepsilon(x)\}$. Thus we have a straightforward algorithm to determine $U(P)$.

Returning once more to the example of Section 2, we trace the execution of GAMMA. Thus $Q = \{2,3,5,7\}$, $R = \{11,13,17,19,23,29\}$, and $x = 37$.

(1) lev = 0, f = "null PCA", f_{max} = "null PCA", $\gamma = 0$

(2) $\beta(x,f) = 23$

(3) $n(1) = 1$, $M(1) = 11$, $RES(1) = 0$

(5) lev = 1, $c(1) = 1$

(6) $f(11) = 0$

(2) $\beta(x,f) = 29$

(3) $n(2) = 1$, $M(1) = 13$, $RES(1) = 9$

(5) lev = 2, $c(2) = 1$

(6) $f(11) = 0$, $f(13) = 9$

(2) $\beta(x,f) = 33$

(3) $n(3) = 0$

(8) $f_{max} = f$, $\gamma = 33$

(9) $c(2) = 2$

(10) lev = 1, $f(11) = 0$

(9) $c(1) = 2$

(10) lev = 0, f = "null PCA"

(11) stop.

Thus the backtrack is very simple in this example. It may, of course, be considerably more complicated.

4. *Applications.*

As indicated in the introduction, the main interest of this author is the evaluation of $U(P_k)$. The author was able to carry out hand calculations of $U(P_k)$ for $k \le 29$ with no difficulty. With a little patience larger sets could also be done by hand. Of course the computer can handle larger sets P.

By computer, we have evaluated $U(P_k)$ for $k < 50$. We tabulate the results in Table 1 below. For $k \ge 23$ we use $Q = \{2,3,5,7\}$ in the evaluation of $U(P_k)$. Thus we considered units modulo 210. This modulus is large enough to keep the amount of backtracking small; for the largest case $(k = 47)$ just over 1 second of computer time was needed to evaluate $\gamma(x)$ for each unit x. However, since there are only 48 units modulo 210, the number of cases which need be considered is also small.

TABLE 1. Values of $U(P_k)$

k	$U(P_k)$	k	$U(P_k)$	k	$U(P_k)$
2	2	13	22	31	58
3	3	17	26	37	66
5	6	19	34	41	74
7	10	23	40	43	90
11	14	29	46	47	100

In Table 2 we indicate how these values can occur, for $23 \le k \le 47$.

We list maximum PCAs, in the same manner as in the example of Section 2.

TABLE 2. Examples Where $U(P_k)$ Is Attained

k	Maximum PCA												
23	67	71	73	79	83	89	97						
	11	13	0	0	0	11	13						
29	191	193	197	199	209	211	221	223	227	229			
	19	17	13	11	0	0	11	13	17	19			
31	187	191	193	197	199	209	211	221	223	227	229	233	
	23	19	17	13	11	0	0	11	13	17	19	23	
37	37	41	43	47	53	59	61	67	71	73	79	83	89
	17	19	23	13	0	0	11	0	17	13	19	11	23
41	179	181	187	191	193	197	199	209	211	221	223	227	229
	31	29	23	19	17	13	11	0	0	11	13	17	19
				233	239	241							
				23	29	31							
43	53	59	61	67	71	73	79	83	89	97	101	103	107
	13	31	11	23	19	17	13	11	0	0	0	0	17
				109	113	121	127	131					
				19	23	31	11	13					
47	41	43	47	53	59	61	67	71	73	79	83	39	97
	31	29	37	13	19	11	23	0	17	13	11	0	19
				101	103	107	109	113	121	127	131		
				29	31	17	0	23	37	11	13		

5. *Final Comments.*

The pattern which occurs for $k = 29$ or 31 can be generalized to give the lower bound $U(P_p) \geq 2q$, where p and q are consecutive primes and $p > q$. In fact, for $p \leq 19$, p prime, maximum PCAs may be obtained in this matter.

The best upper bound we have established is $U(P) \leq 2^{|P|} \prod_{p \in P} \frac{p}{p-1}$.

This is proven by a straightforward application of the inclusion-exclusion principle (see, for example, [1]). We ask what the true order of magnitude of $U(P_k)$ is.

The author intends to establish a bound N_{30} such that $n \geq N_{30}$ guarantees the existence of 30 MOLS of order n. To this end, the result that $U(31) = 58$ is of importance. That is, using the constructions of Wilson [5], it is desirable to have 31 MOLS of various orders in order to perform recursive constructions. This topic will be pursued in a later paper.

REFERENCES

[1] A. E. Ingham, *The Distribution of Prime Numbers*, Hafner Publishing Company, New York, 1971, pp. 10-11.

[2] H. F. MacNeish, *Euler squares*, Ann. Math. *23* (1922), 221-227.

[3] R. C. Mullin, P. J. Schellenberg, D. R. Stinson, and S. A. Vanstone, *On the existence of* 7 *and* 8 *mutually orthogonal Latin squares*, University of Waterloo Research Report *CORR 78-14* (1978), 1-57.

[4] Schilling and Piper, *Basic Abstract Algebra*, Allyn and Bacon, Inc. Boston 1975.

[5] R. M. Wilson, *Concerning the number of mutually orthogonal Latin squares*, Discrete Mathematics *9* (1974), 181-198.

Ohio State University
Columbus 43210

Received September 28, 1978.