MATH 497, MATH 895, CMPT 894.
Assignment 4, Summer 2007

Instructor: Michael Monagan

Please hand in the assignment by 2:30pm on July 18th before class starts.
Late Penalty -20% off for each day late.

REFERENCES

1. *Modern Computer Algebra*, Gerhard and von zur Gathen.
2. Maximal Quotient Rational Reconstruction, M. Monagan.
   Proceedings of ISSAC '2004, ACM Press, 243–249, 2004.

Part (a)

Study Wang's rational number reconstruction algorithm and Monagan's maximal quotient rational reconstruction algorithm (MQRR) in the paper by Monagan. Implement both algorithms in Maple as procedures `Wang` and `MQRR` respectively. For Wang's algorithm, use $N = D = \lfloor\sqrt{m/2}\rfloor$. For Monagan's algorithm, use $T = 1000\lfloor\log_2 m\rfloor$. Execute Wang's algorithm on the following input

```
> m := 23;
> M := floor(sqrt(m/2.0));
> r := [ seq( Wang(u,m,M), u=0..m-1 ) ];
```

Observe that all rationals n/d satisfying $|n| \leq 3$ and $0 < d \leq 3$ appear once in r. Execute Monagan's and Wang's algorithm on the following inputs

```
> p1 := 2^31-1; p2 := prevprime(p1); m := p1*p2;
> U := [ 2/12345678901, 12345678901/2, 123456/78901 ] mod m;
> Digits := 20; M := floor(sqrt(m/2));
> [ seq( Wang(u,m,M), u=U ) ];
> T := 1000*ilog2(m);
> [ seq( MQRR(u,p,T), u=U ) ];
```

The Maple command `ilog2(m)` computes $\lfloor\log_2 m\rfloor$.
The Maple command `iratrecon` does rational number reconstruction.

Part (b)

Let $A \in \mathbb{Z}^{n\times n}$ and $b \in \mathbb{Z}^n$. In class I presented an algorithm for solving $Ax = b$ for $x \in \mathbb{Q}^n$ using linear $p-$adic lifting and rational number reconstruction. Implement the algorithm in Maple as the procedure `padicLinearSolve(A,b)`. Test your implementation on the following examples. The first has large rationals in the solution vector. Print out the number of lifting steps k that are required.

```
> with(LinearAlgebra):
> B := 2^16; m := 3; U := rand(B^m);
> A := RandomMatrix(50,50,generator=U);
> b := RandomVector(50,generator=U);
> x := padicLinearSolve(A,b);
> convert( A.x-b, set ); # should be {0}
> y := [1,0,-1/2,2/3,4,3/4,-2,-3,0,-1];
> x := Vector( [seq( op(y), i=1..5 )] );
> b := A.x;
> b := 12*b; A := 12*A; # clear fractions
> x := padicLinearSolve(A,b);
> convert( A.x-b, set ); # should be {0}
```

To compute $A^{-1} \bmod p$ use `Inverse(A) mod p`.
To multiply A times a vector x use `A.x`.
Your algorithm may be much faster than Maple's LinearSolve routine.

Part (c)

Suppose $\dim A = n$, $\dim b = n$ and $|A_{i,j}| < B^m$ and $|b_i| < B^m$, i.e., the coefficients in the linear system are m base B digits (or less). Suppose the $p - adic$ lifting algorithm does L lifting steps, i.e. solves $Ax = b \bmod p^L$ and then successfully reconstructs $x \in \mathbb{Q}^n$ using rational reconstruction.

What is the running time of the algorithm assuming classical algorithms? Express your answer in the form $O(f(m, n, L))$.

Since the integers in the solution vector x may be as large as mn base B digits, as illustrated by the first example, $L \in O(mn)$ in general. What is the running time for $L \in O(mn)$?

Part (d) Graduate Students Only

Prove the first part of theorem 1 from the paper by Monagan.

Verify that Lemma 1 is true for the data in Table 3 i.e. for $m = 10^6 - 17$ and $u = 137613$.