MACM 442/MATH 800
Makeup Exercise, Fall 2006

Michael Monagan

This makeup question is to be handed in to me by 10:30am Wednesday December 6th.
Late penalty: 10% off for each day late.

If your worst assignment mark is $X/100$, and you get $Y/50$ on this makeup question, I will give you max(100, X+Y) for that assignment.

Makeup Question (50 marks)

Let $n = pq$ where $p \equiv q \equiv 3 \bmod 4$. Recall that the map $f(x) = x^2 \bmod n$ partitions $QR(n)$ into simple cycles. For $n = 192649 = 383 \times 503$ from assignment 5, I found 1 cycle of length 1, 5 cycles of length 50, 2 of length 95 and 50 of length 950.

Explain where the cycle periods 1, 50, 95, 950 come from. Hint: if $x \in QR(n)$ is on a cycle of period π then $x^{2^\pi} \equiv x \bmod p$.

Now explain how p and q can be chosen so that when a user of a BBS generator (who does not know p nor q) chooses the seed s_0 from $QR(n)$ at random, they will get a long cycle with high probability. To answer this, a cycle of period larger than $\sqrt{n}/10$ is long.