9. homework set — Math118, O.Knill

9.1 Given a large number $n = pq$, where p, q are prime numbers, consider the "quadratic map" $T(x) = x^2 + c$ modulo n, where c is an integer. The **Pollard rho method** to factor n looks at the orbit of a point x. Since it will eventually be periodic modulo q, we have $x_n = x_k \bmod q$ which means that $x_n - x_k$ has a common factor with n. Find the orbit structure of the dynamical system $T(x) = x^2 + 1 \bmod n$. Because we have a finite set, every point is eventually periodic. This is the reason for the name ρ. An initial point will eventually be caught in a loop. Find all the periods in the case $n = 15$.

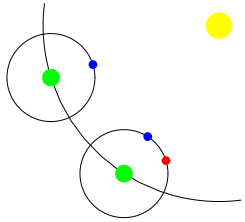
Remark: Assuming the sequence x_n to be random, we need to take about $\sqrt{q}$ iterates to find a factor with probability $1/2$. If you have q different objects and you chose k objects, the probability that two are not the same is $q(q-1)...(q-k+1)/q^k = \frac{q!}{(q-k)!q^k}$. That these probabilities are relatively small is called the **Birthday paradox**. If you have a room of 23 people, then then the probability that two have the same birthday is $1 - 365!/(342!365^23) = 0.5072$. Note that $\sqrt{365} = 19.11...$ is close to 23.

9.2 a) Find the continued fraction expansion of the **golden ratio** $(\sqrt{5}+1)/2$ and relate the periodic approximations p_n/q_n with the Fibonacci sequence.

b) Find the continued fraction expansion of the **silver ratio** $1 + \sqrt{2}$. Can you find the rule, which generates p_n and q_n in the the partial fractions p_n/q_n for the silver ratio?

9.3 A **synodic month** is defined as the period of time between two new moons. It is $\alpha = 29.530588853$ days. The **draconic month** is the period of time of the moon to return to the same node. It is $\beta = 27.212220817$ days. Intersections between the path of the moon and the sun are called **ascending and descending nodes**.

Such an intersection is called a **solar eclipse**. In one approximation, it appears in a period of a bit more then 18 years = 6580 days which is called one **Saros cycle**. This cycle and others are obtained from the continued fraction expansion of α/β. It is said that Thales used the Saros cycle cycle to predict the solar eclipse of 585 B.C. The next big eclipse will happen May 26, 2021. Explain at least two of the following Eclipse cycles (one of them should be the soros cycle) with the continued fraction expansion.



cycle	eclipse	synodic	draconic
fortnight	14.77	0.5	0.543
month	29.53	1	1.085
semester	177.18	6	6.511
lunar year	354.37	12	13.022
octon	1387.94	47	51.004
tritos	3986.63	135	146.501
saros	6585.32	223	241.999
Metonic cycle	6939.69	235	255.021
inex	10571.95	358	388.500
exeligmos	19755.96	669	725.996
Hipparchos	126007.02	4267	4630.531
Babylonian	161177.95	5458	5922.999

If you have no Mathematica installed: turn your browser to

http://sofia.fas.harvard.edu/cgi-bin/sofia

You can get continued fractions by entering something like

ContinuedFraction[Pi, 20].

9.4 We have seen that a parabola $y = p_2(x) = ax^2 + by + c$ defines a dynamical system on the two dimensional torus. This construction goes as follows: $p_1(x) = p_2(x+1) - p_2(x), p_0(x) = p_1(x+1) - p_1(x) = \alpha$ so that $p_1(x+1) = p_1(x) + \alpha$, and $p_2(x+1) = p_2(x) + p_1(x)$. If $x_n = p_1(x+n)$ and $y_n = p_2(x+n)$, then $(x_{n+1}, y_{n+1}) = (x_n + \alpha, y_n + x_n)$.

The curve $f(x) = ax^3 + bx^2 + cx + d$ induces a dynamical system on the three dimensional torus. Find this system and determine whether it preserves area.

9.5 A widely used data encryption technique goes under the name RSA. The security of this encryption is based on the empirical fact that it is hard to factor large integers $n = pq$. Some of the best methods to factor integers goes back to Fermat: assume we can find a second root y of $x^2 \bmod n$, then $x^2 = y^2 \bmod n$ so that $(x-y)(x+y) = 0 \bmod n$ and $gcd(x-y, n)$ is a factor of n. Finding square roots is difficult directly. The **holy grail** is to find numbers y such that $z = y^2 \ mod \ n$ is so small that one can factor them. Having enough such numbers allows to find small squares using a sieaving technique. The Morison-Brillhard method starts with constructing small integers by doing the continued fraction expansion of $\sqrt{n}$. Explain why the periodic approximation $\sqrt{n} \sim p_n/q_n$ produces numbers p_n for which the square p_n^2 is small modulo n. How big do you expect these numbers to be?

Remark. Want to earn 20'000 Dollars? You can do so by factoring the RSA-640 which has 193 digits:

$n = 3107418240490043721350750035888567930037346022842727545720161948823206$
$4405180815045563468296717232867824379162728380334154710731085019195485290073377248227835257423864540146917366024776523466 09.$

See
http://www.rsasecurity.com/rsalabs/node.asp?id=2093
Note that Mathematica has built in factorization techniques. But typing in

FactorInteger[n]

and waiting will most likely will not earn you the prize. Unless you are Indiana Jones ...