On RSA 200 and larger projects

Relatively recent records for NFS factorization are:

- C176, GNFS: K.Aoki Y.Kida T.Shimoyama H.Ueda on May 2, 2005
- C200 (RSA200), GNFS: Bahr Boehm Franke Kleinjung CWI on May 9, 2005
- 911-bit SNFS: K.Aoki Y.Kida T.Shimoyama H.Ueda January 24, 2006

The next interesting steps are the following projects, which mark the limit of what can be done using our software implementation:

- 1024-bit SNFS. Sieving and matrix step are feasible, but organizing the resources for the matrix step may be difficult. The project should be about four times as difficult as RSA200.
- 768-bit GNFS. Sieving is probably feasible, but resources for the matrix step may be very difficult to organize. About 25 times as difficult as RSA200

Polynomial selection for RSA200

Kleinjung-Montgomery-Murphy polynomial selection yielded the following polynomial:

```
#skewness 2766778.76
X5 374029011720
X4 271106563779563011 8
X3 19400071943177513865892714
X2 -338034706092024130946804623603 99
X1 -120887311888241287002580512992469303610
X0 3876720300079932118978295952993877119517096 0
Y1 1272224564842110368688 1
Y0 -375702278070011558966387122336754545 11
M 1524040629812149635455168714947775757996457200705517 74...
0 180000000 3.7 35 100
0 300000000 3.7 35 100
```

Sieving step for RSA200

- Factor base bounds of 300e6 on the algebraic side and 180e6 on the rational side.
- Lattice sieving was done at the BSI and took an estimated 55 CPU years for 2.2 GHz Opteron CPU.
- Lattice sieving was performed for most $q \in [300e6, 1.1e9]$.
- The estimated time for lattice sieving with the an improved siever would have been 37 CPU years.
- Lattice sieving produced a total of 2.6e9 relations.
- 50 million relations from line sieving, done at the CWI and by F. Bahr, were added.
- After removing duplicates 2.26e9 relations remained.

Matrix step for RSA200

- The resulting matrix had 64e6 rows and columns and an average of 171 non-zero coefficients per column.
- Block-Wiedemann was used to produce 128 solutions.
- The step took 3 months on 80 2.2GHz Opterons.

Estimated time for SNFS1024/RSA768

- The sieve step for SNFS1024 is expected to produce 4 times the CPU time for the same number of relations.
- The expected matrix size is 80-130 million.
- A careful prediction of the matrix size should probably be attempted before sieving is started.
- Compared with RSA200, RSA768 might be about 25 times as complicated.
- The Block Wiedemann algorithm may be useful if several institutes want to run the matrix computation in parallel.

Lattice sieving with composite q

It is possible, at the price of getting more duplicates, to sieve with composite numbers as special q: Example c135, all numbers with no prime divisors < 256 accepted as composite special q:

- 700e3 special q produce 23e6 relations with 3.6e6 duplicates.
- We have 87e3 more relations than large primes, the matrix size is 2.5e6, weight 131e6
- 700e3 prime special q yield 22e6 relations with 2.1e6 duplicates.
- We have 300e3 more relations than large primes, the matrix is 2.1e6/144e6.

When some oversieving is done, it is better to also use composite special q:

- 800e3 special q yield 26e6 relations with 4.5e6 duplicates.
- We have 1.1e6 exzess relations, the matrix is 1.5e6/135e6.
- 800e3 special q yield 25e6 relations with 2.7e6 duplicates.
- We have 1.4e6 exzess relations, the matrix is 1.6e6/143e6.

While composite special q should probably be used when oversieving is done to reduce the matrix size, the improvments obtained so far are disappointing.