The pair of sequences (α, β) and one method for the definition of large prime numbers

Emmanuil Manousos

APM Institute for the Advancement of Physics and Mathematics, 13 Pouliou str., 11 523 Athens, Greece

Abstract

In this article, we define a pair of sequences (α, β). By using the properties of the pair (α, β), we establish a method for determining large prime numbers.

Keywords: Number theory, Prime numbers.

2010 Mathematics Subject Classifications: 11A41.

1. Introduction

The determination of big prime numbers is a problem for the number theory, despite the advanced primality tests which are already available [1-5]. In this article we define a pair of sequences (α, β). This pair has specific properties which lead us to a method for the determination of large prime numbers.

2. The pair of sequences (α, β)

We begin our study by the following definitions:

Definition 2.1. *For every prime number P we define as P!!, the product of all prime numbers from 3 to P,*

$$P!!=3\times5\times7\times11\times13\times\ldots\ldots\times P,\ \text{if } P>3 \qquad (2.1)$$

and 0!!=1, 1!!=1, 3!!=3.

Definition 2.2. *For every natural number N we define the pair of sequences (α, β),*

$$\begin{aligned}\alpha&=\alpha(N,P)=2^N-P!!>0\\ \beta&=\beta(N,Q)=Q!!-2^N>0\end{aligned} \qquad (2.2)$$

where P and Q are consecutive prime numbers, P<Q.

From equations (2.2) we get the inequality

$$P!! < 2^N < Q!!. \qquad (2.3)$$

The prime numbers P and Q are consecutive. So, for every natural number N the unique prime numbers P=P(N) and Q=Q(N) of the equations (2.2) are determined from the inequality (2.3). Now, we prove the following theorem.

Theorem 2.1. 1. *The prime numbers which are smaller than P cannot be factors of the sequence α=α(N, P).*

2. *The prime numbers which are smaller than Q cannot be factors of the sequence β=β(N, Q).*

Proof. We prove the theorem for the sequence α. Similarly, the proof for the sequence β can be derived. Every prime number p, $p \le P$, is a factor of P!!. If we suppose that the sequence α has as a factor one of the prime numbers p, then, from the first of the equations (2.2) we have that p is a factor of 2^N, which is not true.□

3. A method for determining prime numbers

There are three reasons for which sequences α and β enable us to determine prime numbers:
a. The numbers α and β are prime numbers if they don't have as a factor any prime number smaller than $\sqrt{\alpha}$ and $\sqrt{\beta}$, respectively. We have, from the theorem 2.1, that the possible prime factors of α and β belong to the intervals $\left(P, \sqrt{\alpha}\right)$ and $\left(Q, \sqrt{\beta}\right)$, and not in $\left[3, \sqrt{\alpha}\right)$ and $\left[3, \sqrt{\beta}\right)$, respectively.

b. For the numbers α and β, a special primality test, as Lucas-Lehmer test for Mersenne numbers, is not required.

c. The number of required trials for the determination of a prime number α or β is extremely low compared to the value of prime α or β.

The method is applied as follows: *We choose a random natural number N. From the inequality (2.3), we determine the consecutive prime numbers P and Q. We apply the primality test in numbers α(N, x), by setting for x the consecutive prime numbers in descending order, beginning from the value x=P. We also apply the primality test in numbers β(N, y), by setting for y the consecutive prime numbers in ascending order, beginning from the value y=Q.*

Next we can see 10 examples.

Example 3.1

For N=976 is P=701 and Q=709.

Sequence α: by doing 2 trials (x=701->691) we get the prime number

α(976, 691)= $2^{976} - 691!! =$

638655 013335 653766 707683 190062 230834 775509 895670 817040 658927 929842 721816 200204 447464 682157 583914 136396 679334 318011 047811 492945 587869

305307 394420 274922 393551 894771 276680 138591 581751 804206 899764 312705 098009 762184 283011 608086 520166 811402 496269 893999 406794 566307 736233 726570 777782 055282 035569 586921 (294 digits).

Sequence β: by doing 25 trials (y=709->719->727->…..->877) we get the prime number

$\beta(976, 877) = 877!! - 2^{976} =$

28383 122954 999577 200045 720963 006112 386644 606569 529211 466652 082580 754370 763953 765906 743384 665027 658538 102868 016012 226390 032854 156811 368648 020398 711626 672440 973533 743831 318966 245752 013255 950936 506997 902874 919004 343796 767713 613210 436243 796431 318422 345245 833886 270164 165216 769019 259548 168967 625580 272879 282877 855051 111182 630154 641134 810004 608533 975807 426263 703310 201419 (365 digits).

Example 3.2

For N=1024 is P=739 and Q=743.

Sequence α: by doing 122 trials (x=739->733->727->.....->29) we get the prime number

$\alpha(1024, 29) = 2^{1024} - 29!! =$

179 769313 486231 590772 930519 078902 473361 797697 894230 657273 430081 157732 675805 500963 132708 477322 407536 021120 113879 871393 357658 789768 814416 622492 847430 639474 124377 767893 424865 485276 302219 601246 094119 453082 952085 005768 838150 682342 462881 473913 110540 827237 163350 510684 586298 239947 245938 479716 304835 356329 620989 290601 (309 digits).

Sequence β: by doing 35 trials (y=743->751->757->…..->983) we get the prime number

$\beta(1024, 983) = 983!! - 2^{1024} =$

9 913869 076957 959363 085476 509349 633687 198817 638885 054873 947070 944907 713208 434521 861169 761377 365943 603383 812227 866097 859307 476964 585620 493484 397944 021856 984574 091662 373772 039115 823054 813289 655134 984555 229299 761650 692165 841668 312889 426532 831892 099786 819659 034378 094642 876612 053735 859107 730567 157931 399224 499912 959067 702770 687512 136579 643647 953901 702116 811745 562127 798029 187108 384116 738749 291148 011773 717375 438449 (409 digits).

Example 3.3

For N=1039 is P=751 and Q=757.

Sequence α: by doing 25 trials (x=751->743->739.....->599) we get the prime number

$\alpha(1039, 599) = 2^{1039} - 599!! =$

5 890680 864316 836766 447387 249177 476247 119386 964598 150177 535756 899376 568524 194361 521975 746399 809212 136563 278436 904792 687334 070508 494811 602620 873366 020549 337847 437121 656499 243581 467969 918332 332162 942962 183137 083602 197379 188445 512607 957222 269672 917213 648347 706862 717030 960392 354633 602163 073301 306617 439423 074080 442133 (313 digits).

Sequence β: by doing 18 trials (y=757->761->769->…..->877) we get the prime number

$\beta(877, 1039) = 877!! - 2\hat{}1039 =$

28383 122954 999577 200045 720963 006112 386644 606569 529205 575971 218263 917604 955235 415780 377477 275679 962111 741031 621839 730352 794946 642970 926295 336819 209045 033152 096191 085848 925771 072111 858886 745528 732553 451966 580868 169633 411418 767043 404774 479882 033826 724619 282574 544851 030377 321618 515780 146696 300119 709730 899953 619202 902032 939830 328470 098143 197982 685569 690847 209958 830667 (365 digits).

Example 3.4

For N=1198 is P=859 and Q=863.

Sequence α: by doing 24 trials (x=859->857->853->.....->701) we get the prime number

$\alpha(1198, 859) = 2^{1198} - 701!! =$

4 304619 864096 437654 516844 424013 158870 894981 186362 172480 433309 204100 175438 923901 347160 699523 554211 731358 974499 882351 306739 203313 218936 786828 545200 906542 600983 180645 013624 913401 057653 956858 671348 516548 856611 241726 487180 916989 111134 698862 757183 903444 720821 025442 328331 214585 842799 152845 212557 233482 277013 840016 424996 937561 460615 787126 116231 096179 660316 412516 378629 (361 digits).

Sequence β: by doing 4 trials (y=863->877->881->883) we get the prime number

$\beta(1198, 883) = 883!! - 2^{1198} =$

2079 884154 217516 230094 729734 187759 542142 573405 492891 585410 215557 034873 660542 246219 198006 437734 277692 629687 558183 450259 209917 465933 562814 065888 160370 150546 070965 836043 171867 838734 314127 810663 262769 996535 624059 479858 246506 401185 237548 950107 058823 197375 964343 994981 306943 188863 686236 600693 299418 674697 473952 457409 195936 042164 534173 190722 963703 940235 571076 329527 638136 133921 (371 digits).

Example 3.5

For N=1233 is P=883 and Q=887.

Sequence α: by doing 4 trials (x=883->881->877->863) we get the prime number

$\alpha(1233, 863) = 2^{1233} - 863!! =$

147905 612271 685434 307673 913194 373664 306503 808919 288997 180748 215878 062902 786084 831112 713161 545678 506968 858167 425839 686482 767218 055846 185820 461117 679299 340529 830802 500988 271828 897627 778074 909866 015483 351305 652186 448177 449187 665452 623203 193558 731565 467821 752030 035357 265365 487387 631047 445872 962623 832457 949353 340203 777614 486145 470418 841974 878490 998052 400973 955992 418360 950377 (372 digits).

Sequence β: by doing 118 trials (y=877->881->883->…..->1721) we get the prime number

$\beta(1233, 1721) = 1721!! - 2^{1233} =$

51 467643 116598 523941 479227 571071 936225 223499 555118 698005 808951 711278 347883 414447 576639 391455 413796 486278 084598 702753 969789 877391 476920 549385 094672 501313 570258 313985 166563 316314 616521 026665 013806 545664 547198 922398 269788 019349 505561 117019 556859 076627 079108 752619 406877 581519 862142 482804 489102 264651 560249 402164 791896 890557 651668 133334 129252 424728 479904 879213 279941 540936 316157 264551 488313 471618 982117 704745 427088 691377 170773 394710 311729 451888 665975 636611 473765 983956 371539 611659 388054 887021 063602 675244 639189 009933 445265 307356 443631 228263 499981 061871 040507 013578 724817 308169 431648 617428 717954 588556 784043 965173 811181 217152 638060 311684 944813 543147 156441 735725 946616 415730 925460 938087 486468 235619 527537 140220 522101 718266 913554 106963 (728 digits).

Example 3.6

For N=1285 is P=929 and Q=937.

Sequence α: by doing 6 trials (x=929->919->911->…..->877) we get the prime number

$\alpha(1285, 877)=2^{1285}-877!!=$

666 107660 458521 541243 186997 828346 474894 176738 104106 101428 036545 819261 386607 628406 990202 569899 466125 164957 129568 678917 571938 657030 735105 124391 574755 325722 042599 216084 491214 928637 323651 676866 603915 434067 911654 598502 970217 278282 233671 705268 345439 289393 732224 716884 248454 195600 756693 342038 634972 546063 505199 471378 881295 089435 538386 411134 264352 553291 275430 652869 419786 211599 575591 216311 537077 (387 digits).

Sequence β: by doing 66 trials (y=937->941->947->…..->1423) we get the prime number

$\beta(1285, 1423)=1423!!-2^{1285}=$

166888 002850 526919 287909 760033 476109 625970 411194 616138 210527 862284 942227 269900 606657 319155 631787 393189 818110 239245 535299 025021 028861 093524 002648 844684 277338 594468 500632 978260 815815 934394 162965 769096 383699 457541 344764 685294 070950 994213 869098 011882 977120 203780 846437 336076 249673 634811 958339 632456 954638 358154 016206 079818 920554 582229 125300 561499 786488 617316 584602 128102 909033 613628 146952 385204 595126 167946 108622 364446 001272 449281 949353 426927 532463 106679 616506 265722 758720 005158 674273 281525 911228 129340 776614 583529 712200 772520 127686 023503 687252 594161 153538 470218 191038 530753 722708 498954 989163 (588 digits).

Example 3.7

For N=2078 is P=1487 and Q=1489.

Sequence α: by doing 16 trials (x=1487->1483->1481->…..->1381) we get the prime number

$\alpha(2078, 1381)=2^{2078}-1381!!=$

34 700121 045228 555050 346908 199627 554351 999626 650564 076873 159288 068873 280937 653055 461604 408140 425567 261849 196041 066352 867645 130420 550233 365566 868443 021761 869796 507131 291564 464848 268224 218371 125990 633413 138622 737136 395894 320752 093994 816268 973831 600772 697147 720354 981623 759476 996479 112473 471981 159382 667244 933804 720126 247366 536062 413797 965111 422507 821264 871777 949707 242888 960408 966701 211391 064073 895954 859365 004395 613211 102351 112369 715672 475962 736556 438519 357829 541892 370016 238257 725210 886762 652866 621267 766904 712807 117086 242981 840932 405810 310119 089665 895656 537293 198835 333031 093149 269553 694775 711411 298044 163997 193083 748629 519229 (626 digits).

Sequence β: by doing 65 trials (y=1489->1493->1499->…..->1993) we get the prime number

$\beta(2078, 1993) = 1993!! - 2^{2078} =$

36 244291 645440 346845 006838 632930 942005 454202 952958 139801 244974 957876 359710 162931 159710 203154 286919 296177 129504 720632 302042 474465 378266 078615 862498 820989 676197 619862 735679 392689 039884 477206 855041 334819 074975 994955 857760 748879 926287 940629 951520 308923 683025 706627 682244 145820 035198 853364 929834 980956 778069 574273 291655 774789 006895 544018 582592 533641 548289 908487 431105 718429 970171 564993 756226 227638 508583 952853 799997 523933 956742 114138 054810 832919 987945 017662 828296 631282 245185 649527 910210 593102 214278 555583 458175 308883 272124 419664 188646 523014 585284 485223 914365 596314 192580 631308 344379 801470 225108 229280 411399 298527 825257 510518 535234 922666 868257 820411 330562 364256 537612 353648 168105 822728 291461 836455 832773 397666 719035 218644 848965 741645 344360 083992 293125 148516 923036 346908 141117 502348 368210 956375 632210 495432 763743 339564 595355 828643 527336 555901 (836 digits).

Example 3.8

For N=2081 is P=1487 and Q=1489.

Sequence α: by doing 92 trials (x=1487->1483->1481->…..->839) we get the prime number

$\alpha(2081, 839) = 2^{2081} - 839!! =$

277 600968 361828 440402 775265 597020 434815 997013 204988 587085 620093 640803 064110 231859 701556 417882 431901 762362 254332 654716 007948 827941 730592 096896 640241 473719 459196 916882 360688 716004 581829 478912 654111 013133 797181 128986 406139 309714 666728 957178 196861 435813 292938 198064 699970 327764 031658 052882 441038 088565 875076 278783 277755 459911 825710 357681 035130 401378 776657 925526 610961 672076 423374 804706 664386 005813 090772 002386 885162 580936 988694 676265 153392 846959 139530 273056 432131 801826 259084 039531 477665 054457 752450 436364 792235 450938 725822 512366 284513 655900 989734 230465 793063 592762 435959 993878 420481 370458 254168 492872 523321 510433 410893 572235 642857 (627 digits).

Sequence β: by doing 5 trials (y=1489->1493->1499->1511->1523) we get the prime number

$\beta(2081, 1523) = 1523!! - 2^{2081} =$

115076 199448 245853 430490 212631 029281 732241 461983 826061 019261 062872 724698 783824 615965 752088 505197 617934 652026 156219 700657 027628 570971 359504 409419 866757 496470 350755 066626 582862 552389 475151 893203 255597 219595 232041 833462 743066 451912 315342 785092 706936 675588 698572 979139 204920 742390 675512 416810 878912 470876 402148 242278 139538 518826 315082 156037 645880 616699 291853 992908 511339 325740 134584 186165 088628 264421 231892 078792 863367 937348 755181 552185 983960 915062 791694 823883 803443 827027 016007 039959 950808 871157 059573 969498 758429 080997 722785 145411 395700 772728 203004 726743 332582 515286 952099 728398 673853 960621 292339 177451 356634 581061 780531 779319 320208 011811 271193 (642 digits).

Example 3.9

For N=3846 is P=2713 and Q=2719.

Sequence α: by doing 52 trials (x=2713->2711->2707->…..->2309) we get the prime number

$\alpha(3846, 2309) = 2^{3846} - 2309!! =$

577249 178684 833827 735902 597536 718890 172894 389921 633305 695751 355401 875472 893117 864892 993286 609538 442868 606594 323864 774731 996158 846914 475490 764195 343753 681516 412315 529115 533701 355853 002097 935773 318297 719238 771780 480723 584223 470389 388611 031809 644063 097166 365934 644074 586968 131721 081074 222442 909233 309219 192527 753937 857414 628446 616545 704302 968941 813293 944685 669936 403358 867038 721099 824419 585396 895665 709897 475394 950607 383244 232888 846760 224470 050201 308152 133952 842671 944071 309160 703843 891564 740268 354314 794911 515197 836061 556715 566605 637417 181306 244851 701738 545168 700932 926236 632602 832089 622719 190053 032458 056011 559595 184222 600539 348254 731922 933652 621953 165906 088227 438709 110645 837804 347290 236185 425112 178165 460149 341362 275713 677028 380956 478681 651276 884469 235980 508491 658395 151398 475662 616528 577224 483546 824075 954261 467489 484604 871017 822270 724269 380133 111994 888168 974369 259418 130357 766581 947161 474819 685759 682905 265169 580943 256658 226400 036499 935793 880975 567970 558175 201291 297021 830307 751265 954045 205398 948332 890994 371540 321543 339889 162045 204248 052055 812085 851877 178521 073782 003369 956423 614252 103784 293424 489641 754260 831716 654312 771917 019917 831475 251319 307111 395619 (1158 digits).

Sequence β: by doing 3 trials (y=2719->2729->2731) we get the prime number

$\beta(3846, 2731) = 2731!! - 2^{3846} =$

112 604900 625801 748310 035114 732534 626270 047845 009963 849599 411051 336655 962418 397928 247108 871336 670082 497317 566372 465722 558250 738773 971184 168212 864202 312061 922653 160358 493857 111102 286997 211890 608191 476341 702417 157626 267293 444427 453307 147943 613123 673500 073354 944973

925822 382910 945283 644875 407200 175949 536283 066697 163993 700139 643381 876694 756084 968089 379066 035886 622184 346596 410231 700416 595849 769162 317175 346547 403983 369700 248123 957391 995391 617894 158302 566895 420462 903278 044021 341159 681986 634693 045230 540603 864751 260827 215477 470552 037003 093585 230544 234584 260267 839256 295135 137906 803958 007985 018988 400689 917229 829510 335407 843139 834747 987355 924309 527083 202453 601894 617559 975954 790146 042423 936716 910334 156815 452978 515057 716637 661841 780815 201808 176490 946478 584115 685236 509474 239847 846386 809158 922947 008636 726873 349973 710595 913563 091149 787611 601529 888143 481408 424940 565545 276808 502079 595951 032962 640950 444923 841382 420958 482377 220563 001544 576241 273302 433790 535535 465111 240779 286060 029741 810753 969927 012132 496819 032629 129430 889817 768920 355777 416160 422502 831338 226045 883796 875640 215876 488399 429671 397626 168217 558948 244697 985644 463749 528487 870042 997564 137312 664838 402004 512004 861381 (1167 digits).

Example 3.10

For N=5000 is P=3539 and Q=3541.

Sequence α: by doing 211 trials (x=3539->3533->3529->…..->1777) we get the prime number

α(5000, 1777)= $2^{5000} - 1777!! =$

141246 703213 942603 683520 966701 614733 366889 617518 454111 681368 808585 711816 984270 751255 808912 631671 152637 335603 208431 366082 764203 838069 979338 335971 185726 639923 431051 777851 865399 011877 999645 131707 069373 498212 631323 752553 111215 372844 035950 900535 954860 733418 453405 575566 736801 565587 405464 699640 499050 849699 472357 900905 617571 376618 228216 434213 181520 991556 677126 498651 782204 174061 830939 239176 861341 383294 018240 225838 692725 596147 005144 243281 075275 629495 339093 813198 966735 633606 329691 023842 454125 835888 656873 133981 287240 980008 838073 668221 804264 432910 894030 789020 219440 578198 488267 339768 238872 279902 157420 307247 570510 423845 868872 596735 891805 818727 796435 753018 518086 641356 012851 302546 726823 009250 218328 018251 907340 245449 863183 265637 987862 198511 046362 985461 949587 281116 578698 456763 034260 464903 435114 174140 916319 217901 928247 416170 291735 036564 790431 283526 480395 934209 315916 242175 763701 184934 468410 303177 096720 672826 883576 656146 896009 875010 355599 449341 010542 696012 007216 719817 555722 774666 219822 118547 841665 704371 214963 760844 783872 967282 603130 046626 015586 763795 760686 152535 117267 709635 551525 698690 103650 762114 449376 403712 991497 506472 076774 255252 494640 368244 829692 969468 147532 357955 822307 845900 787224 345415 972402 197800 943935 589277 413151 592554 543145 793786 121648 378234 203673 835511 875175 567350 494894 785402 885516 143163 018568 787711 998544 494151 407755 504361 029793 832504 584130 049959 371155 973379 999102 979753 617342 852262 692920 052119 004981 034132 526870 876271 505983 856568 155688 297481 270454 614191 389187 087308 659029 454904 596304 943134 597291 (1506 digits).

Sequence β: by doing 195 trials (y=3541->3547->3557->.....->5179) we get the prime number

$\beta(5000, 5179) = 5179!! - 2^{5000} =$

452 337107 134561 064098 997599 885762 545979 204078 658211 395234 815243 457131 254166 899991 956486 623590 273449 294308 223895 007845 233555 632419 838254 915060 364996 618887 342748 353766 324713 619746 478170 682691 209774 062266 595974 118657 224003 860248 517505 912001 163662 509601 930098 299880 552878 471527 216313 511473 803095 533473 812624 972878 102880 712366 881868 620470 058488 893637 795438 496824 498275 959133 293502 323394 717030 289743 265592 253551 016457 554407 705024 236331 049068 547168 339424 844258 107300 787378 208454 939802 286073 728411 799699 757503 623895 110316 009993 259476 136880 042014 096787 442911 604531 438021 561792 285974 995384 083584 153254 239963 419490 335499 951273 518545 616010 528670 547092 484569 087082 803025 289398 602933 183014 370429 997459 344795 852690 369453 722902 994824 369293 346259 598993 613653 754427 995578 890541 091332 019820 845509 701241 983692 552221 595085 568057 812888 833715 788666 100642 018820 415766 638439 683230 751547 262536 472214 390773 995972 628473 954511 721629 342481 870738 713831 580907 244278 808758 273791 286515 875937 396618 118997 968907 994113 686798 608425 560146 047313 647517 654448 015498 911107 356353 113775 213094 743384 028713 371814 370193 966317 136217 249988 108520 615567 463886 767078 324189 224789 448041 708415 943081 585048 063960 728121 951027 280292 802724 860126 627346 846850 419985 094592 672125 283097 828135 264566 777109 274064 634993 811368 984606 528653 412629 261341 577111 696473 625092 406770 655082 325490 635196 356475 360158 642758 938866 354576 067378 559050 357998 247637 107426 748353 926473 583729 134697 153306 909388 022165 763284 419286 725120 443180 126334 449962 271546 869697 867065 080384 426932 312419 561044 813865 280153 420858 214724 216054 367613 457975 310984 994540 415817 037150 617074 890782 326708 859758 078372 696891 129727 753555 210701 784667 022933 304616 727629 468169 615989 843496 991687 919000 771232 171578 508080 379151 111581 337010 996727 727239 777657 999231 821696 440293 418099 892384 059844 454882 542370 226874 304657 876376 409701 576963 605352 387930 713292 733874 198782 524832 120407 510375 046304 054687 250636 922003 711209 934035 695629 831313 275836 285358 390002 253292 653893 395302 070012 448898 932036 836245 468493 465401 704760 417029 591003 856131 981526 943264 925842 376137 902179 239447 319684 379153 017740 622510 757148 229404 731423 068573 213965 129644 542262 468921 042081 389360 136183 577441 309910 193241 012903 556283 190613 204216 123586 070287 948780 339905 396968 063961 699279 (2211 digits).

Nowadays, we know a big number of consecutive prime numbers, so we can calculate extremely high values for P!!. So, by using the pair (α, β) we can determine very big prime numbers. For the sequence α there is an evident limit of trials, approximately P/lnP. However, for the sequence β, we don't have such an evident limit. The properties of the pair (α, β) can be further investigated.

References

[1] Apostol, TomM. *Introduction to analytic number theory*. Springer Science & Business Media, 2013.

[2] Crandall, Richard, and Carl B. Pomerance. *Prime numbers: a computational perspective*. Vol. 182. Springer Science & Business Media, 2006.

[3] Gurevich, Alexander, and Boris, Kunyavskiĭ. "Primality testing through algebraic groups." *Arch. der Math*. 93.6 (2009): 555.

[4] Rempe-Gillen, Lasse, and Rebecca, Waldecker. Primality testing for beginners.*Amer. Math. Soc.*, 2014.

[5] Schoof, René. Four primality testing algorithms.*Algorithmic Number Theory*:*lattices, number fields, curves and cryptography, pp.* 101–126, Math. Sci. Res. Inst. Publ., 44, *Cambridge Univ. Press, Cambridge*, 2008.