

BELL TELEPHONE LABORATORIES
INCORPORATED

THE INFORMATION CONTAINED HEREIN IS FOR
THE USE OF EMPLOYEES OF BELL TELEPHONE
LABORATORIES, INCORPORATED, AND IS NOT
FOR PUBLICATION

COVER SHEET FOR TECHNICAL MEMORANDUM

TITLE — Some Observations on the
Converse of Fermat's Theorem

MM 72 - 1271 - 9

CASE CHARGED — 39199

DATE — October 3, 1973

FILING CASES — 39199-11

AUTHOR LOC. EXT.

Robert Morris MH 2C-524 3878

FILING SUBJECTS — Number Theory

ABSTRACT

A composite pseudoprime is defined as a number that obeys the congruence $2^{p-1} \equiv 1 \pmod{p}$ and yet is not prime. The divisibility and congruence properties of the first 1500 of these numbers reveal some unexpected regularities. Some problems and conjectures are suggested whose solution might bear on the problem of rapid factorization of integers.

NO. OF PAGES — 12

NO. OF REFERENCES — 1

NO. OF TABLES —

NO. OF FIGURES —



Bell Laboratories

Some Observations on the
Converse of Fermat's Theorem
Case 39399-11

October 3, 1972

Robert Morris

MM 72-1271-9

MEMORANDUM FOR FILE

INTRODUCTION

Fermat's theorem states that if p is a prime and a is relatively prime to p , then $a^{p-1} \equiv 1 \pmod{p}$.

A possible converse to Fermat's theorem, which was long believed to be true, is the statement that if $2^{p-1} \equiv 1 \pmod{p}$, then p must be prime. The smallest counterexample to this proposition is the number $341 = 31 \cdot 11$, and there are only 245 such numbers less than one million. Therefore, although this converse to Fermat's theorem is false, there are only a relatively tiny proportion of numbers that disobey it.

A number n that satisfies the congruence $2^{n-1} \equiv 1 \pmod{n}$ is called a pseudoprime (or by some authors, a pseudoprime base 2). The exceptional numbers which disobey the converse can be described as composite pseudoprimes.

Historically, a great deal of interest has been focused on these composite pseudoprimes for the following reasons. First, they are extremely sparse in the integers and even in the pseudoprimes and all of them less than 10 million will fit on one ordinary printed page. Further, it is a much easier matter to test a number for pseudoprimality than to test it for primality. A number n can be tested for pseudoprimality by performing only $\log_2(n)$ multiplications modulo n whereas testing for primality may require the equivalent of $\pi(\sqrt{n})$ divisions. $\pi(k)$ is the number of primes less than k . Of course economies are possible for both methods, but they do not come near to closing the gap in computing times.

For example, a number less than 10 million can be tested for primality by first checking it for pseudoprimality. If it is not a pseudoprime, then by Fermat's theorem it cannot be prime. If it is a pseudoprime then it need only be compared with the one page list of composite pseudoprimes less than 10 million. If it is not on this list, then it is prime.

Before the advent of electronic computers, this scheme was an attractive alternative method, flawed only by the fact that the only existing table of composite pseudoprimes [1] is too inaccurate to be of much use.

More recently, the technique has become less inviting, since on a modern computer, primality can be detected in a matter of milliseconds for numbers as large as 10^{15} and this is far beyond

the range of any table of composite pseudoprimes that could possibly be generated with current techniques.

On the other hand, if restrictions could be put on the possible values of composite pseudoprimes or on their possible divisors, then the pseudoprime approach might again become interesting.

In summary, any theorem about pseudoprimes offers the potential of increasing the speed of testing large numbers for primality. The remainder of this paper is concerned with some empirical observations which lead to the conclusion that there are very strong restrictions on the values of numbers which can be composite pseudoprimes.

A DIGRESSION

An even stronger converse of Fermat's theorem is also false, namely that if $a^{p-1} \equiv 1 \pmod{p}$ for every value of a which is relatively prime to p , then p is a prime. The smallest counterexample to this statement is $561 = 3 \cdot 11 \cdot 17$. On the other hand, a great deal is known about such numbers. They are square-free [2,p.119] and they are the product of at least three primes [1].

NEARLY ALL COMPOSITE PSEUDOPRIMES ARE SQUARE FREE

A check of the first 1500 pseudoprimes showed that all were square-free except for two numbers which were themselves square,

1093^2 and 3511^2 . The numbers 1093 and 3511 are prime and they are the only known primes which satisfy the congruence $2^{p-1} \equiv 1 \pmod{p^2}$. Primes of this sort are of importance in the study of Fermat's Last Theorem. The square of any such prime is a pseudoprime. It is not known whether there are infinitely many such numbers. There are known to be no other such $p < 100,000$ [3].

It is relatively easy to prove [4] that if a pseudoprime is divisible by the square of a prime p , then p^2 is a pseudoprime. There is apparently no other reason to believe that square-free composite pseudoprimes should be particularly sparse or that the only pseudoprimes divisible by a square are themselves square. Among the integers, the square-free integers represent a proportion asymptotically equal to $6/\pi^2$.

not a conjecture
Conjecture 1.: Does the observed excess of square-free pseudoprimes also hold asymptotically?

→ Conjecture 2.: Are all pseudoprimes either square-free or square?

CONGRUENCE PROPERTIES OF PSEUDOPRIMES

The distribution of the first 1500 pseudoprimes among the residue classes mod n was tested for a variety of small n with the following results:

Residue Classes mod 3

= 1 1202
= 2 202
= 0 96

Residue Classes mod 4

= 1 1295
= 3 205

Residue Classes mod 5

= 1 789
= 2 211
= 3 190
= 4 163
= 0 147

Residue Classes mod 7

= 1 552
= 2 155
= 3 172
= 4 130
= 5 160
= 6 155
= 0 176

Residue Classes mod 8

= 1 827
= 3 97
= 5 468
= 7 108

Residue Classes mod 9

= 1 722
= 2 68
= 3 47
= 4 243
= 5 69
= 6 49
= 7 237
= 8 65

Residue Classes mod 11

= 1 336
= 2 110
= 3 112
= 4 108
= 5 132
= 6 111
= 7 100
= 8 123
= 9 110
= 10 126
= 0 132

Residue Classes mod 12

= 1 1034
= 3 5
= 5 170
= 7 168
= 9 91
= 11 32

Residue Classes mod 13

= 1 265
= 2 106
= 3 98
= 4 65
= 5 110
= 6 110
= 7 116
= 8 95
= 9 89
= 10 98
= 11 81
= 12 84
= 0 183

The distribution among these residue classes is most irregular and to each of these moduli there is a large and unexpected surplus of pseudoprimes which have residue 1. The moduli up to 13 have been checked and in each case there is a significant excess of pseudoprimes with residue 1.

The pseudoprimes are all odd numbers by construction but there does not appear to be any other reason why the distribution among residue classes should be irregular. The primes, for example, are known to be distributed evenly among the possible residue classes mod n for every value of n .

Conjecture 3: Does the observed excess of composite pseudoprimes which leave a remainder of 1 for small n hold for all n ?

Conjecture 4: Does the observed excess of composite pseudoprimes which leave a remainder of 1 mod n also hold asymptotically as the number of pseudoprimes increases?

Conjecture 5: Is there any significance to the fact that the number of these pseudoprimes in residue class 1 for prime moduli is very nearly 2.5 times what would be expected?

Robert Morris

Robert Morris

MH-1271-RHM-pdp

Attached
References
Appendix

[1] Poulet, Table des nombres composés vérifiant le théorème du Fermat pour le module 2 jusqu'à 100.000.000

Sphinx 8 (March 1937) 42-52

[2] Shanks, Solved and Unsolved Problems in Number Theory, Vol. I Spartan, 1962.

[3] Kravitz, The congruence $2^{p-1} = 1 \pmod{p^2}$ for $p < 100,000$
Math. Comp. 14 (1960) 378

[4] Lehmer, D. H. On the Converse of Fermat's Theorem
Am. Math. Monthly 43 (1936) 347-354

[5] Hardy & Wright, An Introduction to the Theory of Numbers, 3rd
edition
Oxford, 1954

composite pseudoprimes (base 2)

1	51	101	151	201	251
341	41665	181901	396271	665333	1033669
561	42799	188057	399001	665401	1050985
645	46657	188461	401401	670033	1052503
1105	49141	194221	410041	672487	1052929
1387	49981	196021	422659	679729	1053761
1729	52633	196093	423793	680627	1064053
1905	55245	204001	427233	683761	1073021
2047	57421	206601	435671	688213	1082401
2465	60701	208465	443719	710533	1082809
2701	60787	212421	448921	711361	1092547
2821	62745	215265	449065	721801	1093417
3277	63973	215749	451905	722201	1104349
4033	65077	219781	452051	722261	1106785
4369	65281	220729	458989	729061	1109461
4371	68101	223345	464185	738541	1128121
4681	72885	226801	476971	741751	1132657
5461	74665	228241	481573	742813	1139281
6601	75361	233017	486737	743665	1141141
7957	80581	241001	488881	745889	1145257
8321	83333	249841	489997	748657	1152271
8481	83665	252601	493697	757945	1157689
8911	85489	253241	493885	769567	1168513
10261	87249	256999	512461	769757	1193221
10585	88357	258511	513629	786961	1194649
11305	88561	264773	514447	800605	1207361
12801	90751	266305	526593	818201	1246785
13741	91001	271951	530881	825265	1251949
13747	93961	272251	534061	831405	1252697
13981	101101	275887	552721	838201	1275681
14491	104653	276013	556169	838861	1277179
15709	107185	278545	563473	841681	1293337
15841	113201	280601	574561	847261	1302451
16705	115921	282133	574861	852481	1306801
18705	121465	284581	580337	852841	1325843
18721	123251	285541	582289	873181	1333333
19951	126217	289941	587861	875161	1357441
23001	129889	294271	588745	877099	1357621
23377	129921	294409	604117	898705	1373653
25761	130561	314821	611701	915981	1394185
29341	137149	318361	617093	916327	1397419
30121	149281	323713	622909	934021	1398101
30889	150851	332949	625921	950797	1419607
31417	154101	334153	635401	976873	1433407
31609	157641	340561	642001	983401	1441091
31621	158369	341497	647089	997633	1457773
33153	162193	348161	653333	1004653	1459927
34945	162401	357761	656601	1016801	1461241
35333	164737	367081	657901	1018921	1463749
39865	172081	387731	658801	1023121	1472065
41041	176149	390937	665281	1024651	1472353

composite pseudoprimes (base 2)

301	351	401	451	501	551
1472505	1969417	2513841	3186821	4181921	5131589
1485177	1987021	2528921	3224065	4188889	5133201
1489665	1993537	2531845	3225601	4209661	5148001
1493857	1994689	2537641	3235699	4229601	5173169
1500661	2004403	2603381	3316951	4259905	5173601
1507561	2008597	2609581	3336319	4314967	5176153
1507963	2035153	2615977	3337849	4335241	5187637
1509709	2077545	2617451	3345773	4360621	5193721
1520905	2081713	2626177	3363121	4361389	5250421
1529185	2085301	2628073	3370641	4363261	5256091
1530787	2089297	2649029	3375041	4371445	5258701
1533601	2100901	2649361	3375487	4415251	5271841
1533961	2113665	2670361	3400013	4463641	5284333
1534541	2113921	2704801	3413533	4469471	5310721
1537381	2121301	2719981	3429037	4480477	5351537
1549411	2134277	2722681	3435565	4502485	5400489
1569457	2142141	2746477	3471071	4504501	5423713
1579249	2144521	2746589	3539101	4513841	5444489
1584133	2162721	2748023	3542533	4535805	5456881
1608465	2163001	2757241	3567481	4567837	5481451
1615681	2165801	2773981	3568661	4613665	5489121
1620385	2171401	2780731	3581761	4650049	5489641
1643665	2181961	2793351	3605429	4670029	5524693
1678541	2184571	2797921	3656449	4682833	5529745
1690501	2205967	2811271	3664585	4698001	5545145
1711381	2213121	2827801	3679201	4706821	5551201
1719601	2232865	2867221	3726541	4714201	5560809
1730977	2233441	2880361	3746289	4767841	5575501
1735841	2261953	2882265	3755521	4806061	5590621
1746289	2264369	2899801	3763801	4827613	5599765
1755001	2269093	2909197	3779185	4835209	5632705
1773289	2284453	2921161	3814357	4863127	5672041
1801969	2288661	2940337	3828001	4864501	5681809
1809697	2290641	2944261	3898129	4868701	5733649
1811573	2299081	2953711	3911197	4869313	5758273
1815465	2304167	2976487	3916261	4877641	5766001
1826203	2313697	2977217	3936691	4895065	5804821
1827001	2327041	2987167	3985921	4903921	5859031
1830985	2350141	3020361	4005001	4909177	5872361
1837381	2387797	3048841	4014361	4917331	5919187
1839817	2414001	3057601	4025905	4917781	5968261
1840357	2419385	3059101	4038673	4922413	5968873
1857241	2433601	3073357	4069297	4974971	5977153
1876393	2434651	3090091	4072729	4984001	6027193
1892185	2455921	3094273	4082653	5016191	6049681
1896961	2487941	3116107	4097791	5031181	6054985
1907851	2491637	3125281	4101637	5034601	6118141
1908985	2503501	3146221	4151869	5044033	6122551
1909001	2508013	3165961	4154161	5049001	6135585
1937881	2510569	3181465	4154977	5095177	6140161

composite pseudoprimes (base 2)

601	651	701	751	801	851
6159301	7306261	8719921	10004681	11328409	13421773
6183601	7306561	8725753	10024561	11335501	13446253
6189121	7414333	8727391	10031653	11367137	13448593
6212361	7416289	8745277	10033777	11433301	13500313
6226193	7428421	8812273	10079521	11473885	13554781
6233977	7429117	8830801	10084177	11541307	13635289
6235345	7455709	8902741	10134601	11585293	13635649
6236257	7462001	8916251	10185841	11592397	13694761
6236473	7516153	8927101	10226161	11644921	13696033
6242685	7519441	8992201	10239985	11767861	13747361
6255341	7546981	9006401	10251473	11776465	13757653
6278533	7656721	9037729	10266001	11777599	13773061
6309901	7674967	9040013	10267951	11875821	13823601
6313681	7693401	9046297	10275685	11921001	13838569
6334351	7724305	9056501	10317601	11972017	13856417
6350941	7725901	9063105	10323769	12032021	13899565
6368689	7759937	9069229	10331141	12067705	13942081
6386993	7803769	9073513	10386241	12096613	13971841
6474691	7808593	9084223	10393201	12261061	13991647
6539527	7814401	9106141	10402237	12262321	13992265
6617929	7820201	9131401	10402561	12263131	13996951
6628385	7883731	9143821	10403641	12273769	14012797
6631549	7995169	9223401	10425511	12322133	14026897
6658669	8012845	9224391	10505701	12327121	14154337
6732817	8036033	9273547	10513261	12376813	14179537
6733693	8041345	9345541	10545991	12407011	14282143
6749021	8043841	9371251	10606681	12490201	14324473
6779137	8095447	9439201	10610063	12498061	14469841
6787327	8134561	9480461	10635751	12584251	14556081
6836233	8137585	9494101	10655905	12599233	14589901
6840001	8137633	9533701	10680265	12643381	14609401
6868261	8180461	9564169	10700761	12659989	14671801
6886321	8209657	9567673	10712857	12702145	14676481
6912079	8231653	9582145	10763653	12711007	14684209
6952037	8239477	9585541	10802017	12757361	14709241
6955541	8280229	9588151	10818505	12783811	14794081
6973057	8321671	9591661	10837321	12854437	14796289
6973063	8322945	9613297	10877581	12932989	14865121
6998881	8341201	9638785	10956673	12936763	14870801
7008001	8355841	9692453	10958221	12939121	14885697
7017193	8362201	9724177	10974385	12945745	14892153
7040001	8384513	9729301	10974881	12979765	14898631
7177105	8388607	9774181	11034365	13057787	14899751
7207201	8462233	9816465	11075857	13073941	14913991
7215481	8534233	9834781	11081459	13187665	14980411
7232321	8640661	9863461	11115037	13216141	15082901
7233265	8646121	9890881	11119105	13295281	15101893
7259161	8650951	9908921	11157721	13333441	15124969
7273267	8656705	9920401	11205601	13338371	15139199
7295851	8719309	9995671	11242465	13357981	15162941

composite pseudoprimes (base 2)

901	951	1001	1051	1101	1151
15188557	16973393	19020191	21814417	24158641	27062101
15207361	16998961	19054933	21880801	24161905	27108397
15220951	17020201	19092921	21907009	24214051	27118601
15247621	17098369	19149571	22066201	24356377	27128201
15248773	17116837	19260865	22075579	24726773	27168337
15268501	17134043	19328653	22087477	24776557	27218269
15403285	17208601	19384289	22137809	24904153	27219697
15472441	17236801	19404139	22203181	24913681	27271151
15479777	17316001	19471033	22215961	24929281	27279409
15510041	17327773	19523505	22269745	25080101	27331921
15525241	17375249	19569265	22351249	25150501	27336673
15560461	17405537	19607561	22369621	25266745	27380831
15583153	17429861	19683001	22397497	25270105	27392041
15603391	17450569	19734157	22432201	25276421	27401401
15621409	17509501	19781763	22480381	25326001	27402481
15698431	17585969	19985269	22487101	25457833	27409541
15700301	17586361	20081953	22509691	25520833	27476641
15716041	17590957	20099017	22513457	25540291	27491237
15732721	17641207	20117467	22564081	25557121	27492581
15757741	17698241	20140129	22591301	25603201	27509653
15802681	17759681	20202481	22665505	25629913	27600001
15829633	17777191	20234341	22669501	25640641	27664033
15888313	17812081	20261251	22711873	25696133	27700609
15913261	17870561	20417311	22848541	25768261	27714961
15976747	17895697	20489239	22849481	25831585	27736345
15978007	18003349	20494401	22885129	25840081	27798461
16046641	18007345	20626165	22899097	25846913	27808463
16053193	18067501	20647621	22953673	25873381	27846721
16070429	18073817	20770621	23054601	25909453	27966709
16132321	18137505	20964961	23247901	25947959	27986421
16149169	18151861	20968501	23261713	26254801	28011001
16149601	18162001	21042001	23283037	26280073	28029001
16153633	18300241	21224401	23286781	26296401	28071121
16158331	18307381	21303343	23315977	26377921	28172629
16263105	18366937	21306157	23382529	26465089	28175001
16324001	18443701	21355951	23386441	26470501	28312921
16349477	18454921	21359521	23405341	26474581	28325881
16360381	18468901	21397381	23464033	26553241	28406953
16435747	18487267	21400481	23517985	26634301	28449961
16539601	18490381	21414169	23577497	26719701	28527049
16666651	18535177	21417991	23634181	26758057	28572961
16705021	18541441	21459361	23734901	26813221	28629613
16717061	18595801	21474181	23736385	26821601	28717483
16773121	18607009	21559741	23808721	26840269	28787185
16778881	18653353	21584305	23822329	26877421	29020321
16818877	18736381	21585313	23828017	26886817	29111881
16822081	18740971	21623659	23872213	26921089	29137021
16843009	18779761	21654533	23963869	26932081	29143633
16853077	18900973	21715681	23966011	26977001	29214541
16879501	18985627	21789901	24037021	27032545	29581501

composite pseudoprimes (base 2)

1201	1251	1301	1351	1401	1451
29593159	32368609	36121345	38801089	41590297	44963029
29732221	32428045	36168265	38903287	41604109	45100177
29878381	32497921	36255451	38971661	41607721	45175201
30022129	32676481	36291193	39016741	41642681	45219329
30058381	32701297	36307981	39052333	41662297	45318561
30069721	32756581	36338653	39117439	41840809	45393601
30090817	32899201	36354449	39126313	41866001	45414433
30185569	32914441	36448387	39353665	41987111	45485881
30219757	33018985	36507801	39465091	42009217	45563027
30295141	33146717	36721021	39467377	42344609	45593065
30296761	33193117	36724591	39512773	42485119	45769645
30338593	33298337	36765901	39573073	42490801	45819541
30388753	33302401	36852481	39655153	42623017	45830161
30411201	33408145	36861901	39684157	42689305	45877861
30418957	33596641	36919681	39789841	42694279	45879941
30529693	33600533	36942157	40094341	42697873	45890209
30576151	33627301	36974341	40160737	42702661	46045117
30653245	33704101	36981601	40165093	42709591	46055851
30662497	33840397	37109467	40238797	42763501	46094401
30718441	33848311	37167361	40280065	42984589	46104697
30739969	33872593	37280881	40315441	42998901	46256489
30740417	33965261	37354465	40325041	43039501	46282405
30881551	34003061	37376509	40361197	43136821	46325029
30894307	34043101	37439201	40374901	43224397	46386589
30951181	34100821	37469701	40430401	43235641	46469809
30958201	34111441	37491301	40622401	43286881	46483633
30971161	34124641	37695505	40629601	43331401	46517857
30992401	34196401	37727341	40778989	43363601	46647745
30996001	34386121	37769887	40782589	43397551	46657181
31040833	34487601	37938901	40801861	43584481	46679761
31118221	34540801	37962541	40827473	43620409	46860001
31146661	34581457	37964809	40841821	43661257	46878601
31150351	34603041	37988497	40886241	43798457	47006785
31166803	34657141	38010307	40917241	43914949	47063611
31198693	34856167	38046817	40928701	44070841	47220367
31405501	34890481	38118763	40933705	44081101	47253781
31436123	34901461	38151361	40987201	44238481	47349373
31692805	34944001	38171953	41017681	44314129	47356171
31735621	35428141	38210323	41067665	44347381	47647117
31759121	35498467	38239741	41073241	44465221	47734141
31766983	35571601	38342071	41102601	44472001	47744209
31794241	35576599	38404501	41121433	44482901	47759041
31880577	35626501	38439523	41262073	44521301	47903701
32080651	35703361	38453151	41298985	44671001	47918581
32091781	35820937	38560861	41341321	44695211	47930023
32095057	35851037	38584801	41396921	44731051	47953621
32158621	35926801	38624041	41424801	44823241	48064021
32168117	35932441	38637361	41471521	44824501	48191653
32264029	35967921	38789913	41541241	44912701	48269761
32285041	35976721	38790753	41568101	44953441	48277081