الجمهورية العربية السورية
وزارة التعليم العالي
جامعة البعث
كلية العلوم _ قسم الرياضيات

الخوارزميات الفعالة لتحليل أعداد صحيحة كبيرة

(Efficient algorithms for large integers factorization)

رسالة مقدمة إلى كلية العلوم – جامعة البعث

لنيل درجة الماجستير في المعلوماتية من قسم الرياضيات

إعداد الطالبة

ديما خالد درويش

إشراف

د.محمد النايف الحاج يونس

العام الدراسي:2011- 2010

ملخص الأطروحة

إنّ مسألة تحليل الأعداد الصحيحة إحدى الفروع الهامة في نظريات الأعداد، وفي نظريات حساب تعقيد الخوارزميات وفي الحفاظ على أمن البيانات في الحواسيب من خلال أنظمة التشفير التي تعتمد على دراسات في الأعداد الأولية مثل التحليل إلى عوامل.

والقاعدة الأساسية في الحساب تشير إلى أنه يمكن تحليل أي عدد صحيح إلى عوامل أولية فلتحليل العدد 21 إلى عوامله الأولية نجد ببساطة أنّ $21=3\times7$ ولكن على فرض أنه لدينا عدد كبير مؤلف من خمسة أرقام مثل العدد: $n=11897$ فإنه سيأخذ زمناً للانتهاء من عملية التحليل، لذلك كرسنا اهتمامنا في هذه الرسالة على دراسة أغلبية الخوارزميات الموجودة لتحليل الأعداد الصحيحة، ثم أجرينا العديد من تجارب المحاكاة الحاسوبية لأكثر من ثلاثمائة و ستين عدداً صحيحاً لإجراء مقارنة بين الخوارزميات المدروسة وبعض الخوارزميات المستخدمة في مكتبات برمجية جاهزة منها لغة Matlab بهدف توضيح أداء الخوارزميات المدروسة، ثم رسمنا الخطوط البيانية لتوضيح فعالية كل خوارزمية ومعرفة الأفضل منها .

وقد تبين من التجارب العددية مايلي:

- زمن تنفيذ الخوارزمية Pollard$(p-1)$ هوا لأطول بين جميع الخوارزميات المدروسة.
- زمن تنفيذ الخوارزميةWilliam أكبر من زمن تنفيذ بقية الخوارزميات.
- إن زمن تنفيذ الخوارزمية factor أكبر بقليل من زمن تنفيذ بقية الخوارزميات باستثناء بعض الأعداد .
- زمن تنفيذ خوارزمية Fermat أفضل من زمن تنفيذ خوارزمية Pollard$(p-1)$ وأسوأ من زمن تنفيذ بقية الخوارزميات.

من جهة أخرى، من خلال متابعتنا لتنفيذ الخوارزميات المدروسة على مجموعات الأعداد الصحيحة تبين لنا أن النتائج الحاصلة من تطبيق الخوارزميات المتبقية متقاربة من بعضها، ويمكننا أن نرتب الخوارزميات من الأسوأ إلى الأفضل:

- Pollard$(p-1)$.
- William.
- Factor.
- Fermat
-

Abstract

The integer factorization problem is of the most important parts in the numbers theory, complexity theory, and keeping on security information in computers threw encryption systems that depend on primary numbers like factorization to factors.
The fundamental theorem of arithmetic implies that any composite integer can be factorized, given the number n=21it is straightforward to find the factors of n=21=3*7,Now consider a large number composite of five numbers like number n=11897 it will take a big time to finish factoring operation.
So we take big interest in this thesis on studying the best found algorithms to factor integer numbers, then we do many experiments to over 360 integer numbers to compare ones between studied algorithms and some algorithms in ready programming libraries such as Matlab language in order to explain studied algorithms.Then we drew graph to explain the best know of them .
We have realized threw number experiments:
1- the running time of **pollard(p-1)** algorithm is larger than the running time of other algorithm.
2- the running time of **William** algorithm is larger than the running time of other algorithm.
3- the running time of **factor** algorithm is bigger than the running time of other algorithm except some numbers.
4- the running time of **fermat** algorithm is better than the running time of **pollard(p-1)** algorithm and worse than the running time of other algorithm.

On other hand, threw our interest to execute the studied algorithms on integer numbers.We found that the product results of applicating the remaining algorithms close to us.

Finally:
We can arrange the logarithms from the best to the worst:

- Pollard$(p-1)$.
- William.
- Factor.
- Fermat.